Arithmetically equivalent fields

Lotte van der Zalm

Master thesis Mathematical Sciences, University Utrecht,
Written under supervision of Gunther Cornelissen,
2008

Universiteit Utrecht

Acknowledgements

A thesis, despite appearances, is never created by just one person. Without the moral support and mathematical assistance of many people, this thesis would never have been completed.

In particular, I am deeply grateful to my supervisor, professor Gunther Cornelissen. He helpfully suggested research subjects, and was always willing to help and inspire – even to welcome me at his home when I was completely stuck. I am also indebted to professor Frits Beukers, who fulfilled the nearly-invisible but important role of second reader for this work.

Another word of gratitude is due to my student colleague Joachim Schipper, who proofread my thesis. He pointed out many textual errors and some needlessly opaque passages, and this thesis is a lot better for his work.

I would also like to express my thanks to my friends, Joachim Schipper, Esther Bod, Marte Koning, Willem Maat, Sander Wolters, Ralph van Gelderen, Amarins van de Voorde, Roeland Warringa, Erik Leppen, Wilfred de Bondt, Rob van den Hengel and others, for the shared laughter, for the inspiration, and for the support. I was very happy to share these years with you, and will fondly rememember our time as "het theekransje van de Eigenruimte".

Words cannot express my gratitude to my fiancé Bert Weda. Your love and moral and physical support were a large part of what enabled me to undertake and complete this work.

Last but not least, a word of thanks to my family – Guus and Frouk, Jeroen, Albert and Julia, Hans and Laurenske, and Marieke. Your interest in my work and moral support kept me going.

Abstract

Two number fields K and L are arithmetically equivalent if primes split in K and L with the same inertia degrees. Finite groups H and H' are Gassmann equivalent in $G = \mathrm{Gal}(N/\mathbf{Q})$ if for every $c \in G$, $|c^G \cap H| = |c^G \cap H'|$. In this thesis we prove Perlis' theorem: Number fields K and L are arithmetically equivalent if and only if $\zeta_K(s) = \zeta_L(s)$, which is the case if and only if the Galois groups $H = \mathrm{Gal}(N/K)$ and $H' = \mathrm{Gal}(N/L)$ of the field extensions are Gassmann equivalent, where N is the normal closure of K and L. Additionally, we give two constructions of arithmetically equivalent number fields.

Let M be an abelian number field which is Galois over $\mathbf{Q}$ such that $[K \cap M : \mathbf{Q}] = [L \cap M : \mathbf{Q}]$. We prove that K and L are arithmetically equivalent if and only if KM and LM are arithmetically equivalent. In particular, this is true for quadratic extensions of the number fields K and L. Furthermore, the Artin L-series for any quadratic character is the same in K and L.

Finally, we try to find an analogue to Perlis' theorem which holds over function fields. We show that arithmetical equivalence does not imply equality of the Artin-Weil zeta functions. On the other hand, we also prove that K and L are arithmetically equivalent if and only if their Goss zeta function coincide.

Contents

1 Introduction

In 1880 Kronecker started a new area in number theory. He asked whether a number field could be determined by the way the primes split. This is actually the same question as whether we can determine the number field by the zeta function.

For a number fields K and a prime number p, let us assume that p splits in K as

$$p = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_k^{e_k}.$$

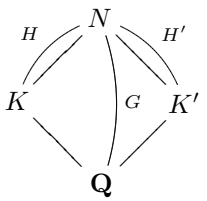
In this formula k is the number of different primes which *lie above* the prime p and e_i are the corresponding *ramification indices*. If we now order the primes such that the *inertia degrees* $f_i = [\mathcal{O}_K/\mathfrak{p}_i : \mathbf{Z}/p]$ of these primes form a non-decreasing sequence, we say that this sequence of inertia degrees is the *splitting type* of the prime p.

The study of arithmetically equivalent fields gives us the answer to Kroneckers question. We call two fields *arithmetically equivalent* if all primes have the same splitting type in both fields, but the fields are non-isomorphic.

If two fields are arithmetically equivalent then the number fields do have certain properties in common. For example: the Dedekind zeta function, the discriminant, the unit group, the class number times the regulator, the normal closure, etc.

The triple (H, H', G) is a *Gassmann triple* if H and H' are subgroups of G and for all conjugacy classes of G the overlapping with H respectively H' have an equal number of elements.

Let K and K' be two number fields, and let N be a Galois extension of both K and K'. Denote by G (respectively H, H') the Galois group of N over $\mathbf{Q}$ (respectively K, K' over $\mathbf{Q}$). Gassmann proved that K and K' are arithmetically equivalent if and only if the triple (H, H', G) is a Gassmann triple.



The other characterization of arithmetically equivalence of number fields are that their Dedekind zeta function is equal. In the 18th century Leonhard Euler studied the Basel problem: find the exact value of the series $\zeta(2) = \sum_{n\geq 0} \frac{1}{n^2}$. In 1735 he found the solution $\zeta(2) = \pi^2/6$, and also the solutions for $\zeta(4), \zeta(6), \zeta(8), \zeta(10)$ and $\zeta(12)$. Two years later he found the famous relation between the series and the Euler product of the prime numbers

$$\zeta(s) = \sum_{n\geq 0} \frac{1}{n^s} = \prod_{p \text{ prime}} \left(1 - p^{-s}\right)^{-1}.$$

He also found that for positive n the equalities $\zeta(-n) = -\frac{B_{n+1}}{n+1}$ and $\zeta(-2n) = 0$, where B_n are the Bernoulli numbers.

More than a century later Georg Friedrich Bernhard Riemann examined more closely the zeta function of Euler. But Euler had described it as a real function and he wanted to consider it as a complex function. Riemann studied the convergence of the zeta function and found

$$\zeta(s) / \left((2\pi i)^{r_1 s}\right)^2 \in \mathbf{Q}.$$

We call the zeros $-2n$ which Euler found the trivial zeros. Riemann proved that all non-trivial zeros of $\zeta(s)$ have a real part between 0 and 1. After some research he stated his famous hypothesis, which is still one of the most important unsolved problems of mathematics. It states that the nontrivial zeros are all on the line $\mathrm{Re}(s) = 1/2$.

Dirichlet thought that this zeta function could be generalized to the zeta function over quadratic extensions of $\mathbf{Q}$ in stead of $\mathbf{Q}$. In this case we take the sum over the norms of the ideals of this quadratic extension. This definition is generalized by Dedekind to a general number field K and is called the Dedekind zeta function:

$$\zeta_K(s) = \sum_{\substack{I \subset \mathcal{O}_K \\ \text{nonzero}}} \frac{1}{\mathcal{N}_{K/\mathbf{Q}}(I)^s}$$

where $\mathcal{N}_{K/\mathbf{Q}}$ is the product of all conjugates of the ideal the extension K over $\mathbf{Q}$, the conjugates are the elements of the Galois group. Note that if we take the number field $\mathbf{Q}$, we obtain the Riemann zeta function. The Dedekind zeta function has a meromorphic continuation to the complex plane such that it has only poles $s = 0$ and $s = 1$. There is also a functional equation connecting $\zeta_K(s)$ with $\zeta_K(1 - s)$. Furthermore for $s > 1$ it has no zeros, by the functional equation the zeta function vanishes to a certain order for negative integers s.

In this thesis the theory of arithmetically equivalent over number fields will be described in chapter 2. It shows that two arithmetically equivalent number fields are also Gassmann equivalent and induce the same Dedekind zeta function. We give in chapter 3, explicit examples of two different number fields for which the corresponding zeta function is equal. Hence we are talking about fields which really occur. Thirdly, we look what happens if we extend these number fields. If two fields are arithmetically equivalent are their extensions still arithmetically equivalent? For a "nice" extension, the corresponding zeta functions turn out to be equal, as proven in chapter 4.

In chapter 5 we describe the relationship between the Dedekind zeta functions and the Artin L-series $\zeta_{K(\sqrt{d})}(s) = \zeta_K(s)\mathcal{L}(N/K, \chi, s)$. If K and K' are arithmetically equivalent and χ is a quadratic character the corresponding Artin L-series $\mathcal{L}(N/K, \chi, s)$ and $\mathcal{L}(N/K', \chi, s)$ are equal.

Because the results of Perlis and of the extensions are mainly based on some group theoretical facts, the question arises whether these results are still true for zeta functions defined over function fields, which are "similar" to number fields. A function field $\mathbf{F}_q(t)$ is a finite field $\mathbf{F}_q$ together with a transcendental element t over $\mathbf{F}_q$.

The zeta function over function fields can be defined in different ways. We will start with the classical definition of the zeta function over function fields. The classical zeta function over function fields was introduced and studied by Artin and Weil. They thought of the norm as the number of residue classes, which turned out to be $q^{\deg(D)}$, where D is a divisor of $\mathbf{F}_q(t)$. The Artin-Weil zeta function, is given by

$$\zeta_K(s) = \sum_D \mathcal{N}(D)^{-s},$$

where the sum ranges over the positive divisors D of $\mathbf{F}_q(t)$. The Riemann hypothesis turns out to be true for this zeta function.

The Artin-Weil zeta function has become very simple, it is just a rational function of q^{-s}. Thereby, this zeta function does not contain enough information about

our field. We can not say as much about the underlying fields as in the number field case. This issue is described in chapter 6. Therefore we have to consider a "better" zeta function over function fields.

The Carlitz zeta function is a zeta function over function fields which is based on a more natural definition of the norm. It remains more information because its norm n is defined in characteristic p. This norm does not give a value in $\mathbf{Z}$, but in our ground field, the function field K. The Carlitz zeta function, defined for $s \in \mathbf{Z}$, is given by:

$$\zeta_{\mathcal{O}_K} = \sum_{I \subset \mathcal{O}_K} \frac{1}{n(I)^s}$$

In this function we have to take the power of an ideal. Luckily Goss found a way to extend the definition to more than just integers. He defined a "new" complex plane by taking the direct product of p-adic integers and some completion of our ground field. In this way he gets an extension of taking the power of an integer to taking the power of an ideal. This is described in chapter 6.3.

This zeta function does indeed keeps much more information about the underlying field. And we can indeed construct a complete analogue of the theory about arithmetically equivalent number fields. We can reconstruct the old proof, because the classical proof of Perlis' theorem depends mostly on some group theoretically facts.

Last but not least, some "nice" extensions of function fields do also keep the property of arithmetical equivalence.

2 Introducing arithmetic equivalence

The Dedekind zeta function over a number field K is a complex analytic function from which we can extract significant information about our number field. The zeta function is defined as:

$$\zeta_K(s) = \sum_{\substack{I \subset \mathcal{O}_K \\ \text{nonzero}}} \mathcal{N}_{K/\mathbf{Q}}(I)^{-s}$$

In this chapter we first give some statements which can be derived from basic group theory. Secondly, we discuss the translation of these group-theoretic statements to the Galois group of a number field. After this, we prove Perlis' theorem on arithmetically equivalent number fields, which gives a number of statements equivalent to the equality of two zeta functions.

2.1 Group theory

In this paragraph we define the notion of coset type and Gassmann equivalence. We will show that equal coset types and Gassmann equivalence are two equivalent notions. First we take a finite group G, a subgroup $H \subset G$ and a cyclic subgroup $C \subset G$. Let τ_i for $i = 1, \dots h$ be a representatives of the double cosets $H\backslash G/C$, so $G = \bigcup_{i=1}^{h} H\tau_i C$.

Definition 2.1. *The* coset type *of (G, H, C) is a tuple $A = (f_1, \dots, f_h)$ of integers defined by $|H\tau_i C| = |H| \cdot f_i$, where the f_i are ordered such that $f_i \leq f_{i+1}$.*

Definition 2.2. *Two subgroups H and H' of a finite group G are* Gassmann equivalent *if $|c^G \cap H| = |c^G \cap H'|$ for all conjugacy classes $c^G = \{gcg^{-1} | g \in G\}$. In this case we have the Gassmann triple (H, H', G).*

Lemma 2.3. (Gassmann) *Two subgroups H and H' of a finite group G are Gassmann equivalent if and only if for all cyclic subgroups $C \prec G$ the coset types of (G, H, C) and (G, H', C) coincide.*

Proof. We first prove that both Gassmann equivalence and equal coset types imply $|H| = |H'|$.
"Gassmann equivalent $\Rightarrow |H| = |H'|$": If two conjugacy classes, say c^G and d^G, overlap, then there are $\sigma, \tau \in G$ such that $\sigma c \sigma^{-1} = \tau d \tau^{-1}$, so $c = \sigma^{-1}\tau d (\sigma^{-1}\tau)^{-1}$, giving $c^G \subset d^G$, hence these conjugacy classes are equal. For an arbitrary $h \in H$, we have $h^{\mathrm{Id}} = h$, so the conjugacy classes cover H. Hence $H = \dot{\bigcup}_{\substack{c \in G \\ \text{repr.}}} (c^G \cap H)$, i.e. H is a disjoint union of representatives of conjugacy classes intersected with the subgroup H. Thus we have

$$|H| = \sum_{\substack{c \in G \\ \text{repr.}}} |c^G \cap H| = \sum_{\substack{c \in G \\ \text{repr.}}} |c^G \cap H'| = |H'|.$$

"Equal coset types $\Rightarrow |H| = |H'|$": We have $f_i = f_i'$ for all $i \in \{1, \dots, h\}$ where the f_i and f_i' are given by

$$|H\tau_i C| = |H| \cdot f_i \text{ and } |H'\tau_i' C| = |H'| \cdot f_i'.$$

Because $G = \bigcup_{i=1}^{h} H\tau_i C = \bigcup_{i=1}^{h} H'\tau_i' C$ we can deduce

$$|G| = |H| \cdot \sum_{i=1}^{h} f_i = |H'| \cdot \sum_{i=1}^{h} f_i,$$

hence $|H| = |H'|$.

By defining numbers l_i which depend on the coset type, we can make numbers k_i which depend on the Gassmann equivalence class. Let C be an arbitrary cyclic subgroup of G, and let c be its generator. Define the number l_i:

$$\begin{aligned} l_i &= |\{g \in G : |HgC| = |H| \cdot i\}| \\ &= |\{\text{cosets of } HgC : \text{order is } |H| \cdot i\}| \cdot |H| \cdot i \end{aligned}$$

This last equation holds because each coset of order $|H| \cdot i$ has exactly $|H| \cdot i$ elements. Define the number k_i

$$\begin{aligned} k_i &= \sum_{d|i} l_d \\ &= |\{g \in G : |HgC| \text{ divides } |H| \cdot i\}| \\ &\overset{(1)}{=} |\{g \in G : |C^g|/|H \cap C^g| \text{ divides } i\}| \\ &\overset{(2)}{=} |\{g \in G : H \cap \langle c\rangle^g \supseteq \langle c^i\rangle^g\}| \\ &\overset{(3)}{=} |\{g \in G : gc^i g^{-1} \in H\}| \\ &= |(c^i)^G \cap H| \cdot |\text{stabilizer of } c^i|. \end{aligned}$$

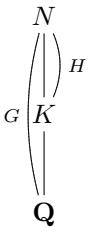
(1) Because $|HgC| = |HgCg^{-1}| = |HC^g| = |H| \cdot |C^g|/|H \cap C^g|$.
(2) The order divides i, so for an arbitrary $a \in C^g$ we have $a^i \sim 1$ in $C^g/(H \cap C^g)$, and thus $a^i \in (H \cap C^g)$. Actually, we have $\langle c^i\rangle^g \subseteq H \cap \langle c\rangle^g$.
(3) Since $g\langle c\rangle^i g^{-1} \subseteq g\langle c\rangle g^{-1} = \langle c\rangle^g$ we can simplify $\langle c^i\rangle^g \subseteq (H \cap \langle c\rangle^g)$ to $g\langle c\rangle^i g^{-1} \subset H$. Because H is a group it is enough to only require this for the generator.

Now Möbius inversion (c.f. [LS92]) gives us $l_i = \sum_{d|i} k_d \mu(i/d)$, where μ is the classical Möbius function. Analogously, we get l_i' and k_i' for the group H'.

We have defined l_i respectively l_i' in such a way that we have that if for all cyclic groups C the coset types are equal if and only if $l_i = l_i'$ for all i (by $|H| = |H'|$). By the last part of the proof we have $l_i = l_i'$ for all i if and only if $k_i = k_i'$ for all i. The number k_i respectively k_i' is equal to the number of elements of the conjugates of c^i which are in H respectively H' times the number of elements which stabilizes c^i. Because the last part of this definition is equal for k_i and k_i' we get that we have $k_i = k_i'$ for all i if and only if $|(c^i)^G \cap H| = |(c^i)^G \cap H'|$ for all i, and this defines Gassmann equivalence for H and H'. □

2.2 Number fields

In this paragraph we want to translate the notions of the previous paragraph to number fields. We do this by taking a Galois extension of our number field and by considering the Galois group G. We will show that the coset type of these groups actually tells us how a prime splits in our extension.



Let K be an arbitrary number field and let N be an finite extension of K which is Galois over $\mathbf{Q}$ with Galois group G. Furthermore let H be the Galois group of this extension, i.e. $H = \mathrm{Gal}(N/K)$, which is a subgroup of G.

Definition 2.4. *The* decomposition group G_P *of a prime ideal $P \subset N$ is the set*

$$\{\sigma \in G \mid \sigma P = P\}.$$

The inertia group *is a subgroup of the decomposition group and it consists of the elements of the decomposition group which are the identity on the the residue class of the prime, i.e.*

$$I_P = \{\sigma \in G \mid \forall \omega \in \mathcal{O}_P : \sigma\omega \equiv \omega \ (mod\ \mathfrak{P}).$$

The decomposition group G_P of a prime ideal P which lies unramified above a prime number $p \in \mathbf{Z}$ is isomorphic to $\mathrm{Gal}(\mathcal{O}_N/P, \mathbf{F}_p)$ by the map sending $\sigma \in G_P$ to the map $\overline{a} \mapsto \overline{\sigma a}$ (for $a \in \mathcal{O}_N$), where $\overline{a}$ means a modulo P. This Galois group is cyclic, so for unramified primes the decomposition group is cyclic.

Now we can define the splitting type of the prime number p:

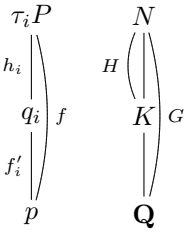
Definition 2.5. *The* splitting type $A = (f'_1, \ldots, f'_g)$ *of a prime number $p \in \mathbf{Z}$ in K is given by the inertia indices $f'_i = [\mathcal{O}_K/P_i : \mathbf{Z}/p]$ of the primes $P_i|p$, where the inertia indices are ordered by $f'_i \leq f'_{i+1}$.*

The next theorem is from Hasse, described in paragraph 23 of [Has30].

Theorem 2.6. (Hasse) *Let K be a number field and let N be a finite extension Galois over $\mathbf{Q}$ with Galois group $H = Gal(N/K)$ and $G = Gal(N/\mathbf{Q})$. Let p be a prime number which splits unramified in N and let P be a prime of N above p. Let G_P be a decomposition group of P. Furthermore let A' denote the splitting type of p in K, and let A denote the coset type of (G, H, G_P). Then $A = A'$.*

Proof. As before, we can write G in the following way

$$G = \bigcup_{i=1}^{h} H\tau_i G_P.$$



The prime number p splits in K into $p = q_1 \ldots q_g$. The group H acts transitive on the set of primes which lies above a certain prime q_i. Let τ_i be such that $\tau_i P$ lies above some q_i. Because elements of G_P fix P, $\tau_i G_P P$ also lies above q_i. Furthermore elements of H fix q_i, so $H\tau_i G_P P$ lies above q_i. If there is another $\tau'_i \in G$ such that $\tau'_i P$ lies above q_i, then by transitivity of the action of H on the primes above a certain prime of K there exists a $v \in H$ such that $\tau'_i P = v\tau_i P$. Hence $\tau'_i = v\tau_i\zeta$ for some $\zeta \in G_P$. Thus $p = \prod_i q_i$ and $q_i = \prod_{\tau'_i \in H\tau_i G_P} \tau'_i P$. Note that since p is unramified in N our original union is disjoint, so $G = \dot{\bigcup}_{i=1}^{g} H\tau_i G_P$.

Let f be the inertia degree of N over $\mathbf{Q}$. Note that this does not depend on our choice of p because N is Galois over $\mathbf{Q}$. Let h_i be the inertia degree of N over K of the prime $\tau_i P$ over q_i and let f_i' be the inertia degree of K over $\mathbf{Q}$ of the prime q_i over p. Then $f = f_i' h_i$ for all $i \in \{1, \ldots, g\}$.

We get $G_{\tau_i P} = \tau_i G_P \tau_i^{-1}$: For an arbitrary $\sigma \in G_P$ we have $\tau_i \sigma \tau_i^{-1}(\tau_i P) = \tau_i P$. The number of elements of the decomposition group is equal to the inertia degree of the prime, i.e. $f = |G_{\tau_i P}| = |G_P|$. Furthermore, as $q_i = \prod_{\tau \in H\tau_i G_P} \tau P$ we find $h_i = |H_{\tau_i P}| = |H \cap G_{\tau_i P}|$.

Putting this together we get:

$$\begin{aligned} |H| \cdot f_i &= |H\tau_i G_P| \\ &= |H\tau_i G_P \tau_i^{-1}| \\ &= |H G_{\tau_i P}| \\ &= |H| \cdot \frac{|G_{\tau_i P}|}{|H \cap G_{\tau_i P}|} \\ &= |H| \cdot \frac{f}{h_i} \\ &= |H| \cdot f_i' \end{aligned}$$

Hence $A = A'$. □

There is an interesting corollary, but we will need some definitions. Denote the set of primes which have the same splitting type A by

$$P_K(A) := \{p \in \mathbf{Z} \text{ of splitting type } A \text{ in } K\}.$$

We will also use $D \doteq E$ to signify that the sets D and E differ only by a finite number of elements, i.e. almost all elements are equal.

We briefly restate the Chebotarev density theorem (see also [SJ96]). The density of S (a subset of the set of unramified primes) is given by:

$$\delta(S) = \lim_{N \to \infty} \frac{\{p \in S : p \leq N\}}{\{p \text{ prime} : p \leq N\}}$$

Let the *cyclic pattern* of an element σ in G be the ordered lengths of the disjoint permutation cycles of σ. Chebotarev states that for a cyclic subgroup $C \subset G$ with a generator of cyclic pattern A, the density of $P_K(A)$ is equal to $|C|/|G|$.

Corollary 2.7. *The coset type of (G, H, C) and of (G, H', C) are equal for all cyclic subgroups C if and only if $P_K(A) \doteq P_{K'}(A)$ for all A.*

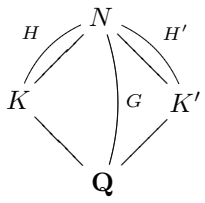
Proof. Only finitely many primes are ramified. The decomposition group G_P of an unramified prime is a cyclic group. Hence for finitely many primes the decomposition group is cyclic. If for all cyclic subgroups C the coset types coincide, then this is in particular true for the decomposition groups. Theorem 2.6 gives us that the coset types are the same as the splitting type of this prime, so we get

$$P_K(A) \doteq P_{K'}(A) \quad \text{for all } A.$$

The converse also holds. Every cyclic subgroup C with a generator of cyclic pattern A consist of elements with the same cyclic pattern. By the Chebotarev density theorem, every group C is a decomposition group for infinitely many primes. Assume that the splitting type of the primes in K and K' is equal except for finitely many primes. Now, since $f_i = f_i'$ we have that the coset types coincide. □

2.3 Theorem on arithmetically equivalent number fields

Perlis' theorem gives some equivalent statements of arithmetically equivalent number fields. It also gives some properties of these underlying number fields. But first we give a lemma which we need for the proof of this theorem.



Lemma 2.8. *Let K and K' denote two number fields, not necessarily Galois over $\mathbf{Q}$. Take an arbitrary finite Galois extension N of both K and K' over $\mathbf{Q}$ and denote its Galois group by G. Note that $H = Gal(N/K)$ and $H' = Gal(N/K')$ are subgroups of G. Let n and m be in $\mathbf{N}$. Define the following functions for $s \in \mathbf{C}$:*

$$\begin{aligned} \tau_1(s) &= \prod_{j=1}^{n}(1-c_j^{-s}) \quad \text{for } c_j \in \mathbf{R}_{>1} \\ \tau_2(s) &= \prod_{j=1}^{m}(1-d_j^{-s}) \quad \text{for } d_j \in \mathbf{R}_{>1} \\ \tau(s) &= \frac{\tau_1(s)}{\tau_2(s)} \end{aligned}$$

Let $f(s)$ be a meromorphic function with zeros and poles not equal to the zeros and poles of either $\tau_1(s)$ or $\tau_2(s)$. If $f(s)$ satisfies:

$$\tau(s) = f(s)\tau(1-s)$$

Then $\tau_1(s) = \tau_2(s)$ and $f(s) = 1$.

Proof. We may assume that no c_i is equal to any of the d_j. Otherwise we can just divide out the common factors in τ_1 and τ_2. By definition τ_1 and τ_2 are holomorphic functions with zeros $\left\{\frac{2\pi ik}{\log c_j}\right\}$ for $k \in \mathbf{Z}$ and $j = 1, \ldots, n$, respectively $\left\{\frac{2\pi ik}{\log d_j}\right\}$ for $k \in \mathbf{Z}$, and $j = 1, \ldots, m$.

Let $s_0 = \frac{2\pi ik}{\log c_1}$, which is a zero of $\tau_1(s)$. Now $1 - s_0$ is not a zero of $\tau_1(s)$, because if it were a zero, then $1 - \frac{2\pi ik}{\log c_1} = \frac{2\pi ik}{\log c_j}$ for some $j \in \{2, \ldots, n\}$ and $k, k' \in \mathbf{Z}$. This gives us:

$$1 = 2\pi i\left(\frac{k}{\log c_1} + \frac{k'}{\log c_j}\right)$$

which is a contradiction. Obviously, the same line of reasoning works for τ_2. By assumption f has different zeros as $\tau_1(s)$, so $f(s_0)$ is nonzero.

Because $\frac{\tau_1(s)}{\tau_2(s)} = \tau(s_0) = f(s_0)\tau(1-s_0) \neq 0$, we need $\tau_2(s_0) = 0$. Note that this means that for a certain j_1 we have $c_1^{s_0} = d_{j_1}^{s_0} = 1$ which means that $c_1 = d_{j_1}^{k_1}$ for some $k_1 \in \mathbf{Z}$.

By setting $c_{j_1} = c_1$ this can be rewritten as $d_{j_1} = c_{j_1}^{k_1}$. Since $c_{j_1}, d_{j_1} > 1$, the integer k_1 has to be positive. Similarly, setting $s_1 = \frac{2\pi i}{\log d_{j_1}}$ gives $c_{j_2} = d_{j_1}^{l_1}$ for some positive l_1. We repeat this process until we get a repetition in the j_i's. Since there are only n distinct numbers c_j this gives a relation:

$$c_{j_i} = c_{j_i}^{k_i l_i \ldots k_{i+s} l_{i+s}}$$

where k_i and l_i are strictly positive, so $k_i = l_i = \cdots = k_{i+s} = l_{i+s} = 1$. But then $c_{j_i} = d_{j_i}^{k_i} = d_{j_i}$, so $\tau_1(s)$ and $\tau_2(s)$ have a common factor, which is in contradiction

with the assumption that we divided them all out. Hence $\tau(s)$ is equal to a constant. Taking the limit for s going to infinity, we find that this constant is equal to 1. Hence $\tau_1(s) = \tau_2(s)$ and $f(s) = 1$. □

Before we state the theorem on arithmetically equivalent number fields we need one extra definition about number fields.

Definition 2.9. *The* normal core *of K is the largest subfield of K which is normal over* $\mathbf{Q}$.

Definition 2.10. *Two fields are* arithmetically equivalent *if all $p \in \mathbf{Z}$ have the same splitting type, i.e. if for every tuple A we have $P_K(A) = P_{K'}(A)$.*

Theorem 2.11. Perlis' theorem *Let K and K' be two number fields, and let N be an extension of both K and K', which is Galois over $\mathbf{Q}$. Then the following statements are equivalent:*

(a) $\zeta_K(s) = \zeta_{K'}(s)$;

(b) The number fields K and K' are arithmetically equivalent;

(c) For every tuple A we have $P_K(A) \doteq P_{K'}(A)$;

(d) $H = Gal(N/K)$ and $H' = Gal(N/K')$ are Gassmann equivalent.

If one of these statements is true then all of the following hold:

1. *$[K : \mathbf{Q}] = [K' : \mathbf{Q}]$;*
2. *The discriminants of K and K' are equal;*
3. *The number of real valuations of K and K' are equal;*
4. *K and K' have the same normal closure;*
5. *K and K' have the same normal core;*
6. *The unit groups U_K and $U_{K'}$ are isomorphic.*

Proof. "(a) ⇒ (b)": Define

$$\begin{aligned} A(n) &= |\{I \subset \mathcal{O}_K : \mathcal{N}_{K/\mathbf{Q}}(I) = n\}| \\ A'(n) &= |\{I \subset \mathcal{O}_{K'} : \mathcal{N}_{K'/\mathbf{Q}}(I) = n\}|. \end{aligned}$$

Now $\zeta_K(s) = \sum_{n\in\mathbf{N}} \frac{A(n)}{n^s}$ and $\zeta_{K'}(s) = \sum_{n\in\mathbf{N}} \frac{A'(n)}{n^s}$ for $\mathrm{Re}(s) > 1$. Thus

$$A(1) = \lim_{s\to\infty} \zeta_K(s) = \lim_{s\to\infty} \zeta_{K'}(s) = A'(1).$$

Let us suppose $A(i) = A'(i)$ for all $i = 1, \ldots, l-1$. Now cancel the terms $A(i)$ respectively $A'(i)$ in the zeta functions and multiply this with l^s. The limit for s going to infinity gives the following equality

$$A(l) = \lim_{s\to\infty} \sum_{n\geq l} \frac{A(n)}{n^s} \cdot l^s = \lim_{s\to\infty} \sum_{n\geq l} \frac{A'(n)}{n^s} \cdot l^s = A'(l) \quad \forall l \in \mathbf{N},$$

so this is true for all $l \in \mathbf{N}$. In $\mathcal{O}_K$ and $\mathcal{O}_{K'}$ every nonzero prime ideal is maximal. To consider only the prime ideals we have to subtract all the non-maximal ideals. Let $B(p^f)$ be the number of prime ideals of norm p^f, hence

$$B(p^f) = A(p^f) - \sum_{\substack{a_1+\cdots+a_t=f \\ a_i\in\mathbf{N}, t\geq 2}} A(p^{a_1}) \ldots A(p^{a_t}).$$

Now $B(p^f)$ determines the splitting type of p in K. We can define $B'(p^f)$ analogously and $B(p^f = B'(p^f)$. It follows that $P_K(A) = P_{K'}(A)$.

"(b) $\Rightarrow$ (c)": This is trivial.

"(c) $\Leftrightarrow$ (d)": By corollary 2.7 we have for every tuple A that $P_K(A) \doteq P_{K'}(A)$ if and only if the coset types of (G, H, C) is equal to the coset type of (G, H', C) for all cyclic subgroups C of G. Secondly, lemma 2.3 gives that we have equal coset types if and only if H and H' are Gassmann equivalent.

"(d) $\Rightarrow$ (a)": In this case C is the decomposition group of the real infinite divisor of $\mathbf{Q}$, i.e. either C consists only of the identity or C has also complex conjugation, so this group C is cyclic. Let $n_1(K)$ respectively $n_1(K')$ be the number of real valuation of the number field K respectively K'. Now

$$n_1(K) = |\{Ht_iC : |Ht_iC| = |H|\}| = n_1(K'),$$

because by (d) and the proof of lemma 2.3 we have $|H| = |H'|$. Similarly, let $n_2(K)$ respectively $n_2(K')$ be the number of complex valuations of K respectively K', then

$$n_2(K) = |\{Ht_iC : |Ht_iC| = 2|H|\}| = n_2(K').$$

Define

$$\begin{aligned} G_1(s) &= \pi^{-s/2}\Gamma\left(\frac{s}{2}\right), \quad G_2(s) := (2\pi)^{1-s}\Gamma(s) \\ Z_K(s) &= G_1(s)^{n_1(K)}G_2(s)^{n_2(K)}\zeta_K(s). \end{aligned}$$

As described in [Neu92], the completed zeta function Z_K is analytic outside 0 and 1 and $Z_K(s) = |D_K|^{(1/2)-s}Z_K(1-s)$, where D_K and $D_{K'}$ are the corresponding discriminants.

Since the real and complex valuations are equal for K and K', it follows that:

$$\frac{\zeta_K(s)}{\zeta_{K'}(s)} = \frac{Z_K(s)}{Z_{K'}(s)} = \left|\frac{D_K}{D_{K'}}\right|^{(1/2)-s} \cdot \frac{\zeta_K(1-s)}{\zeta_{K'}(1-s)}$$

The zeta function has an Euler product $\zeta_K(s) = \prod_{P\subset K}(1 - N(P)^{-s})^{-1}$ for $\mathrm{Re}(s) > 1$. Since we have (c) if and only if we have (d), we know that there are only finitely many primes which have a different splitting type. Hence the quotient of the zeta functions of K and K' is a finite product:

$$\frac{\zeta_K(s)}{\zeta_{K'}(s)} = \frac{\prod_{j=1}^{m}(1 - d_j^{-s})^{-1}}{\prod_{j=1}^{n}(1 - c_j^{-s})^{-1}}$$

By analytic continuation this is true for all complex s. We get by lemma 2.8, $\zeta_K(s) = \zeta_{K'}(s)$.

Let us now proof the properties of arithmetically equivalent number fields K and K'.

"(1)": This is obvious as $|H| = |H'|$ and

$$|H| \cdot [K : \mathbf{Q}] = [N : K][K : \mathbf{Q}] = [N : \mathbf{Q}] = [N : K'][K' : \mathbf{Q}] = |H'| \cdot [K' : \mathbf{Q}],$$

hence $[K : \mathbf{Q}] = [K' : \mathbf{Q}]$.

"(2)": Lemma 2.8 gives us $\left|\frac{D_K}{D_{K'}}\right| = 1$ and hence $D_K = (-1)^{n_2(K)}|D_K|$. Because the complex valuations of K and K' are equal, the discriminants are also equal.

"(3)": This follows from the proof of (d) implies (a).

"(4)": The normal closure of $K/\mathbf{Q}$ is equal to the fixed field of

$$\bigcap_{\sigma\in G} H^\sigma = \{g \in G \mid \forall \sigma \in G : \sigma^{-1} g \sigma \in H\},$$

which indeed contains K. Take $h \in \bigcap_{\sigma\in G} H^\sigma$. For all $\sigma \in G$, $\sigma h \sigma^{-1} \in H$, so by (d) $|h^G| = |h^G \cap H| = |h^G \cap H'|$. Thus $h \in \bigcap_{\sigma\in G} H'^\sigma$. Likewise $\bigcap_{\sigma\in G} H'^\sigma \subset \bigcap_{\sigma\in G} H^\sigma$, so $\bigcap_{\sigma\in G} H^\sigma = \bigcap_{\sigma\in G} H'^\sigma$.

"(5)": The normal core of K is the fixed field of $\langle H^\sigma | \sigma \in G\rangle$. For all $h \in H$, $h^{\mathrm{Id}} \in H$, so $|h^G \cap H'| = |h^G \cap H| \neq 0$. It follows that there exist a $\sigma \in G$ such that $h^\sigma \in H'$. This is true for each h, and the analogue is true for all $h' \in H'$. Thus we have an inclusion of the generators. Hence $\langle H^\sigma | \sigma \in G\rangle = \langle H'^\sigma | \sigma \in G\rangle$.

"(6)": By Dirichlet's unit theorem the unit group is a direct product of a free group and a finite cyclic group generated by the largest root of unity of K resp. K'. This free group has rank $n_1(K) + n_2(K) - 1$ resp. $n_1(K') + n_2(K') - 1$, which are equal because the valuations are equal. Adjoining a generating root of unity ζ of K to $\mathbf{Q}$ ($\mathbf{Q}(\zeta)$) is a normal extension which lies in K' by (5). Likewise the roots of unity of K' lie in K, so K and K' have the same roots of unity, hence the unit groups are isomorphic. □

3 Construction of arithmetically equivalent fields

In this chapter we will discuss two constructions of arithmetically equivalent number fields, i.e. two non-isomorphic number fields which induce the same Dedekind zeta function. This construction is based on the theory of cohomology of groups, which will be introduced in the first paragraph. A general construction will be given. We will work out the details for a specific example. Finally, we discuss a simpler construction for number fields of which the Galois group is a subgroup of a symmetric group.

3.1 Cohomology of finite groups

Before we can prove the lemmas necessary for this construction we need some basic facts from the theory of cohomology of groups. We will give some definitions and the relation between them. For more details we refer to the literature, e.g. [Wei69], [CF67b], [HS00] page 183-190 or [Sil86] page 330-337.

Let G be a finite group and let A be a G-module. Let α^σ be the image of α under the action of $\sigma \in G$. It is often interesting to look at the largest submodule on which G acts trivially

$$H^0(G,A) = \{a \in A \mid \forall \sigma \in G : a^\sigma = a\}.$$

Obviously the short exact sequence of G-modules $0 \to A \xrightarrow{\iota} B \xrightarrow{\kappa} C \to 0$ induces the exact sequence

$$0 \to H^0(G,A) \xrightarrow{\iota_0} H^0(G,B) \xrightarrow{\kappa_0} H^0(G,C).$$

This sequence is not necessarily right exact anymore. To make this right exact we need to look at the maps from G to A with some special properties, the so-called *group of 1-cocycles*

$$Z^1(G,A) = \{\phi : G \to A \mid \forall \sigma,\tau \in G : \phi(\sigma\tau) = \phi(\sigma)^\tau + \phi(\tau)\}.$$

This is a group under addition, where $(\phi+\psi)(\sigma) = \phi(\sigma) + \psi(\sigma)$. Obviously $\phi : G \to A;\ \sigma \mapsto 1$ is the unit. Note that A is abelian, so for $\phi, \psi \in Z^1(G,A)$

$$\begin{aligned}(\phi+\psi)(\sigma\tau) &= \phi(\sigma)^\tau + \phi(\tau) + \psi(\sigma)^\tau + \psi(\tau)\\ &= \phi(\sigma)^\tau + \psi(\sigma)^\tau + \phi(\tau) + \psi(\tau)\\ &= (\phi+\psi)(\sigma)^\tau + (\phi+\psi)(\tau).\end{aligned}$$

Thus $Z^1(G,A)$ is closed under addition. Furthermore, the inverse of $\phi \in Z^1(G,A)$ is $-\phi$ (A is a group, so A contains inverse elements). Finally,

$$(\phi + (\psi+\chi))(\sigma) = \phi(\sigma) + (\psi+\chi)(\sigma) = \phi(\sigma) + (\psi(\sigma) + \chi(\sigma)),$$

so the group is associative as A is. Likewise, it is abelian, because A is abelian.

Some of these cocycles are actually *coboundaries*, i.e.

$$B^1(G,A) = \{\phi : G \to A \mid \exists a \in A : \forall \sigma \in G :\ \phi(\sigma) = a^\sigma - a\}.$$

It is straightforward to see that $B^1(G,A) \subset Z^1(G,A)$. We can do this by taking an arbitrary $\phi \in B^1(G,A)$. From the definition of a coboundary we know that there exists an $a \in A$ such that $\phi(\sigma) = a^\sigma - a$ for all $\sigma \in G$. Consequently,

$$\phi(\sigma\tau) = a^{\sigma\tau} - a = a^{\sigma\tau} - a^\tau + a^\tau - a = (a^\sigma - a)^\tau + (a^\sigma - a),$$

and hence $\phi \in Z^1(G,A)$.

Actually the coboundaries form a subgroup of the cocycles. We have $0 \in B^1(G,A)$ by taking $a = 0$. And for $\phi, \psi \in B^1(G,A)$, there are $a, b \in A$ such that

$$(\phi + \psi)(\sigma) = \phi(\sigma) + \psi(\sigma) = a^\sigma - a + b^\sigma - b = (a+b)^\sigma - (a+b),$$

which is again a coboundary, so $B^1(G,A)$ is closed under addition. The inverse map of ϕ is $\phi^{-1}(\sigma) = -\phi(\sigma) = -(a^\sigma - a) = (-a)^\sigma - (-a)$, which is indeed a coboundary. Hence $B^1(G,A)$ is a subgroup of $Z^1(G,A)$, and it is in fact a normal subgroup because $Z^1(G,A)$ is abelian.

Now we define the first cohomology group by

$$H^1(G,A) = Z^1(G,A)/B^1(G,A).$$

We would like to show that this gives an extension of our exact sequence.

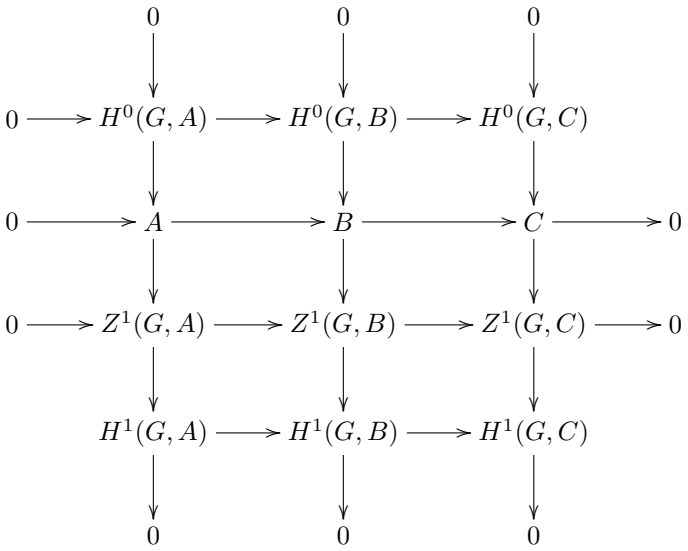
Proposition 3.1. *Let A, B and C be G-modules and let $0 \to A \xrightarrow{\iota} B \xrightarrow{\kappa} C \to 0$ be a short exact sequence, where ι and κ are G-homomorphisms. This induces the following long exact sequence*

$$0 \to H^0(G,A) \xrightarrow{\iota_0} H^0(G,B) \xrightarrow{\kappa_0} H^0(G,C) \xrightarrow{\delta} H^1(G,A) \xrightarrow{\iota_1} H^1(G,B) \xrightarrow{\kappa_1} H^1(G,C).$$

Proof. By definition we have the following exact sequence

$$0 \to H^0(G,A) \xrightarrow{\iota} A \xrightarrow{f} Z^1(G,A) \xrightarrow{p} H^1(G,A) \to 0,$$

where i is just the inclusion of $H^0(G,A)$ in A, and the map f sends $a \in A$ to $a^\sigma - a$, so obviously $\ker(f) = H^0(G,A)$. Furthermore p is the canonical projection map, so $\mathrm{im}(f) = B^1(G,A) = \ker(p)$. We have analogous exact sequences for B and C. This gives the following commutative diagram:



By the snake lemma we get the following long exact sequence

$$\begin{aligned} 0 \quad \to \quad & H^0(G,A) \to H^0(G,B) \to H^0(G,C) \\ & \to H^1(G,A) \to H^1(G,B) \to H^1(G,C). \end{aligned}$$

Let H be a subgroup of G. Now we can define the restriction map: □

Definition 3.2. *The* restriction map $\mathrm{Res}_{G/H}$ *from G to H is a homomorphism from $H^1(G,A)$ to $H^1(H,A)$ restricting cocycles in $H^1(G,A)$ to H, yielding cocycles in $H^1(H,A)$. If it is obvious which groups are involved, we usually omit the subscript.*

This map is well-defined, because the restriction map sends a coboundary of $\phi \in H^1(G,A)$ to $\phi|_H$, a coboundary of $H^1(H,A)$.

Let $G = \bigcup_{i=1}^{n} \sigma_i H$ be a left coset decomposition. Define the *trace* of A from H to G to be $N_{G/H}(a) = \sum_{i=1}^{n} a^{\sigma_i}$ for $a \in H^0(H,A)$ (note $\sum_{i=1}^{n} a^{\sigma_i} \in H^0(G,A)$). This map is a homomorphism because

$$N_{G/H}(a+b) = \sum_{\sigma \in H} (a+b)^{\sigma} = N_{G/H}(a) + N_{G/H}(b).$$

Let us again consider the exact sequence introduced in proposition 3.1:

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\kappa} C \to 0.$$

Now define the *corestriction* $\mathrm{Cor}_{G/H} : H^1(H,A) \to H^1(G,A)$ by demanding that the following diagram (from the long exact sequence) is commutative:

$$\begin{array}{ccccc} \cdots \longrightarrow & H^0(H,C) & \xrightarrow{\delta_H} & H^1(H,A) & \longrightarrow \cdots \\ & \downarrow{\scriptstyle N_{G/H}} & & \vdots{\scriptstyle \mathrm{Cor}} & \\ \cdots \longrightarrow & H^0(G,C) & \xrightarrow{\delta_G} & H^1(G,A) & \longrightarrow \cdots \end{array}$$

For an arbitrary $c \in C$ there exist a $b \in B$ such that $\kappa(b) = c$, because the map κ is surjective. Note

$$\delta_H(c) = \{h \mapsto \iota^{-1}(b^h - b) | h \in H\}.$$

Furthermore,

$$(\delta_G \circ N_{G/H})(c) = \delta_G \left(\sum_{i=1}^{n} c^{\sigma_i} \right) = \{g \mapsto \iota^{-1}(b^g - b) \mid g \in G\}.$$

This gives the following natural definition of the corestriction:

Definition 3.3. *The* corestriction map $\mathrm{Cor}_{G/H}$ *from $H^1(H,A)$ to $H^1(G,A)$ is induced by the map $N_{G/H}$, it sends ϕ to $\{g \mapsto \sum_{i=1}^{n} \phi(\pi(g))^{\sigma_i}\}$, where π projects G on H by sending every element to its coset representative. When it is obvious which groups are meant, we usually omit the subscript.*

This map is well-defined. If we take another representative σ_j' instead of σ_j, then $\sigma_j H = \sigma_j' H$, so $\sigma_j' \sigma_j^{-1} \in H$. Furthermore, for all $h \in H$ we have:

$$\phi(h)^{\sigma_j'} - \phi(h)^{\sigma_j} = \left(\phi(h)^{\sigma_j' \sigma_j^{-1}} - \phi(h) \right)^{\sigma_j}$$

which is a coboundary. It is also a 1-cocycle

$$\begin{aligned}
\mathrm{Cor}(\phi)(g_1g_2) &= \sum_{i=1}^{n} \phi(\pi(g_1g_2))^{\sigma_i} \\
&= \sum_{i=1}^{n} \phi(\pi(g_1))^{\sigma_i\pi(g_2)} + \phi(\pi(g_2))^{\sigma_i} \\
&\overset{(1)}{=} \sum_{i=1}^{n} \phi(\pi(g_1))^{\sigma_i g_2} + \phi(\pi(g_2))^{\sigma_i} \\
&= \sum_{i=1}^{n} (\phi(\pi(g_1))^{g_2} + \phi(\pi(g_2)))^{\sigma_i} \\
&= N_{G/H}(\phi(g_1)^{g_2} + \phi(g_2)) \\
&= N_{G/H}(\phi(g_1))^{g_2} + N_{G/H}(\phi(g_2)) \\
&= \mathrm{Cor}(\phi)(g_1)^{g_2} + \mathrm{Cor}(\phi)(g_2),
\end{aligned}$$

where (1) holds because all $\sigma_i g_2$ are representatives of $\pi(g_2)$, and hence g_2 is also a representative of $\pi(g_2)$. This map is even a homomorphism, because for arbitrary $\phi, \psi \in H^1(H, A)$ we have

$$\begin{aligned}
\mathrm{Cor}(\phi+\psi) &= \{\tau \mapsto N_{G/H}((\phi+\psi)(\pi(\tau)))\} \\
&= \{\tau \mapsto N_{G/H}(\phi(\pi(\tau))) + N_{G/H}(\psi(\pi(\tau)))\} \\
&= \mathrm{Cor}(\phi) + \mathrm{Cor}(\psi).
\end{aligned}$$

This gives rise to the following lemma:

Lemma 3.4. *For any $x \in H^n(G, A)$ we have $\mathrm{Cor}_{G/H} \circ \mathrm{Res}_{G/H}(x) = [G : H] \cdot x$.*

Proof. We have the left coset decomposition $G = \bigcup_{i=1}^{n} \sigma_i H$. For each σ_i, we get a copy of x, because for some $g, g' \in G$ such that $\pi(g) = \pi(g')$ we have $\sum_{\sigma_i} x(\pi(g))^{\sigma_i} = \sum_{\sigma_i} x(\pi(g'))^{\sigma_i}$. □

Definition 3.5. *Let A be an H-module. A is an* induced H-module *if it is isomorphic to $\mathbf{Z}[H] \otimes_{\mathbf{Z}} X$, where X is an abelian group on which H acts trivially.*

Definition 3.6. *The* Augmentation ideal *I of the group ring $\mathbf{Z}[H]$ is the kernel of the map from $\mathbf{Z}[H]$ to $\mathbf{Z}$ defined by sending $\sum_{h\in H} n_g g \mapsto \sum_{h\in H} n_g$. This gives the short exact sequence*

$$0 \to I \to \mathbf{Z}/n[H] \to \mathbf{Z}/n \to 0.$$

We will need another lemma, which we give here without proof. First, let $I_H = \ker\{\mathbf{Z}[H] \to \mathbf{Z}\}$.

Lemma 3.7. (c.f. [CF67b])
Let H be a cyclic group and A an H-module. Then $H^1(H, A) = \ker(N_{H/1})/I_H A$.

Lemma 3.8. *Let H be a cyclic group and A be a finite induced H-module. Then $H^1(H, A) = 0$.*

Proof. Consider the following exact sequence

$$0 \to H^0(H, A) \to A \xrightarrow{T} A \to A/(I_H A) \to 0.$$

Let h be the generator of H. The map T sends any $a \in A$ to $a^h - a$, so by definition $H^0(H, A) = \ker(T)$. Furthermore, we need $\mathrm{im}(T) = I_H A$. To check this we first

observe that $\mathrm{im}(T) \subseteq I_H A$. For the other inclusion we have $\ker(N_{H/1}) \subseteq \mathrm{im}(T)$, because $N_{H/1}$ sends a to $\sum_{i=1}^{n} a^{h^i}$, where $n = |H|$. Note that H is cyclic, so $h^n = 1$. Now

$$N_{H/1}(T(a)) = \sum_{i=1}^{n} a^{h^{i+1}} - \sum_{i=1}^{n-1} a^{h^i} = a^{h^{n+1}} - a^h = 0.$$

Additionally $I_H A \subseteq \ker(N)$, because if we take an arbitrary $a = \sum_{i=0}^{n-1} a_i^{h^i} \in I_H A$, then $\sum_{i=0}^{n-1} a_i = 0$ and we get

$$N(I_H A) = \sum_{i=1}^{n} a^{h^i} = \sum_{i=1}^{n} \sum_{j=0}^{n-1} a_j^{h^{i+j}} \overset{(1)}{=} \sum_{k=0}^{n-1} \sum_{l=0}^{n-1} a_l^{h^k} = 0,$$

where (1) is because h^n is the trivial action. It follows that

$$I_H A \subseteq \ker(N) \subseteq \mathrm{im}(T) \subseteq I_H A,$$

and hence $I_H A = \mathrm{im}(T)$. Therefore this sequence is indeed exact, and hence $|H^0(H, A)| = |A/(I_H A)|$.

We also have $H^1(H, A) = \ker(N_{H/1})/(I_H A)$ (by lemma 3.7) and the following exact sequence

$$0 \to \ker(N_{H/1})/(I_H A) \to A/(I_H A) \xrightarrow{N_{H/1}} H^0(H, A) \to H^0(H, A)/N(A) \to 0.$$

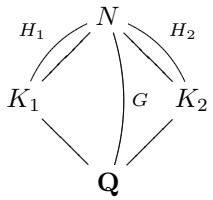
Hence $|H^1(H, A)| = |H^0(H, A)/N_{H/1}(A)|$.

By definition $A \cong \mathbf{Z}[H] \otimes_{\mathbf{Z}} X$, so every element of A can be uniquely written as $\sum_{\sigma \in H} \sigma \otimes x_\sigma$. If this element is H-invariant, i.e. $\sum_{\sigma \in H} \tau\sigma \otimes x_\sigma = \sum_{\sigma \in H} \sigma \otimes x_\sigma$ for every $\tau \in H$, then all x_σ are equal in $H^0(H, A)$, so every element can be written as $N_{H/1}(1 \otimes x) \in N_{H/1}(A)$, giving us $H^0(H, A) \subset N(A)$. Hence $H^1(H, A) = 0$. □

Definition 3.9. *A* principal homogeneous space *over a group G is a set X on which G acts regularly (i.e. transitive and free).*

3.2 Construction by split group extension

In this paragraph, we want to construct two fields K_1 and K_2 which are arithmetically equivalent. They are obtained as the fixed fields of the subgroups H_1 and H_2 of the Galois group $G = \mathrm{Gal}(N/\mathbf{Q})$.



Since K_1 and K_2 are non-isomorphic their Galois groups (the corresponding subgroups of G) are not conjugate in G. In this construction they will appear as representatives of a group H. The *split group extension* $A \rtimes H$ of A by H, is the Cartesian product of A and H with the operation $(a_1, h_1) \star (a_2, h_2) = (a_1 a_2^{h_1}, h_1 h_2)$. We will start with a *split exact sequence*, i.e. an exact sequence,

$$1 \to A \xrightarrow{\iota} G \xrightarrow{\kappa} H \to 1,$$

where there exists a *cut* $\sigma : H \to G$ such that $\kappa \circ \sigma = \mathrm{Id}_H$ and G is a split group extension of a multiplicatively written abelian group A by H. Hence $G \cong A \rtimes H$, where H acts on A by $a^h = gag^{-1}$ for any $h \in H$ and $a \in A$ and an arbitrary $g \in \kappa^{-1}(h)$. Denote by M the equivalence classes of the cuts:

$$M = \{\sigma : H \to G \mid \kappa \circ \sigma = I_H\}/\sim$$

where $\sigma \sim \tau$ if and only if there exist an $a \in A$ such that for all $h \in H$ we have $\sigma(h) = a \cdot \tau(h) \cdot a^{-1}$.

The action of $H^1(H, A)$ on M is defined for $x \in H^1(H, A)$ by taking an arbitrary 1-cocycle $\chi : H \to A$ of x

$$[\sigma] \to {}^x[\sigma] := [\chi \cdot \sigma],$$

where $(\chi \cdot \sigma)(h) := \chi(h) \cdot \sigma(h)$. This is a well-defined action, because it is independent of the choice of representatives in x and in $[\sigma]$. For example let $\chi \in x$ and $\sigma, \tau \in [\sigma]$; then there exists an $a \in A$ such that $\sigma(h)a = a\tau(h)$ for all $h \in H$. Indeed

$$(\chi \cdot \sigma)(h)a = \chi(h)\sigma(h)a = \chi(h)a\tau(h) = a\chi(h)\tau(h) = a(\chi \cdot \tau)(h),$$

and hence $\chi \cdot \sigma \sim \chi \cdot \tau$. Now let $\overline{\chi} \in x$ be another representative of x, so there exists an $a \in A$ such that

$$\chi(h)^{-1}\overline{\chi}(h) = a^h a^{-1} = \sigma(h)a\sigma(h)^{-1}a^{-1} \quad \forall h \in H, \sigma \in M.$$

Hence

$$(\chi \cdot \sigma)(h)a = \chi(h)\sigma(h)a = \overline{\chi}(h)a\sigma(h) = a\overline{\chi}(h)\sigma(h) = a(\overline{\chi} \cdot \sigma)(h) \quad \forall h \in H,$$

so $\chi \cdot \sigma \sim \overline{\chi} \cdot \sigma$. The action is free; if we take an $x \in H^1(H, A)$ which acts trivially on $[\sigma] \in M$, i.e. $[\sigma] = {}^x[\sigma] = [\chi \cdot \sigma]$ for some representative $\chi \in x$, then there exists an $a \in A$ such that $a(\chi \cdot \sigma)(h) = \sigma(h)a$. So

$$\chi(h) = a^{-1}\sigma(h)a\sigma(h)^{-1} = a^{-1}a^h,$$

which is a coboundary, and hence $x = 1$.

Lemma 3.10. *Let H, A and M be as above. Then M is a principal homogeneous space over $H^1(H, A)$. In particular $|M| = |H^1(H, A)|$.*

Proof. Look at 3.9 for the definition of a principal homogeneous space. Our defined action is the morphism we need. We saw before that this action is free.

To see that this action is also transitive, let $[\sigma]$ and $[\tau]$ be two arbitrary classes in M. Now define the map

$$\chi : H \to A; \quad \chi(h) = \tau(h)\sigma(h)^{-1}.$$

Indeed $\kappa(\chi(h)) = \kappa(\tau(h)\sigma(h)^{-1}) = \kappa(\tau(h)) \cdot j(\sigma(h)^{-1}) = 1 \cdot 1 = 1$, so $\chi(h) \in A$. This is a 1-cocycle because

$$\begin{aligned}
\chi(hg) &= \tau(hg)\sigma(hg)^{-1} \\
&= \tau(h)^g\tau(g)(\sigma(h)^g\sigma(g))^{-1} \\
&= \tau(h)^g\tau(g)\sigma(g)^{-1}(\sigma(h)^g)^{-1} \\
&= \tau(g)\tau(h)\tau(g)^{-1}\tau(g)\sigma(g)^{-1}(\sigma(g)\sigma(h)\sigma(g)^{-1})^{-1} \\
&= \tau(g)\tau(h)\sigma(h)^{-1}\sigma(g)^{-1} \\
&= \tau(g)\tau(h)\sigma(h)^{-1}\tau(g)^{-1}\tau(g)\sigma(g)^{-1} \\
&= (\tau(h)\sigma(h)^{-1})^g\tau(g)\sigma(g)^{-1} \\
&= \chi(h)^g\chi(g).
\end{aligned}$$

Let $x \in H^1(H, A)$ be the class containing this χ. Now ${}^x[\sigma] = [\tau]$, so our action is transitive. Hence $H^1(H, A)$ acts regularly on M.

Because the action is transitive and free we also have $|M| = |H^1(H, A)|$. □

Let us consider the subgroup $\langle h\rangle$ of H for any $h \in H$, now we get the induced exact sequence

$$1 \to A \xrightarrow{\iota} G_h \xrightarrow{\kappa} \langle h\rangle \to 1,$$

where G_h is the pre-image of $\langle h\rangle$. Similarly M_h is the equivalence class of cuts restricted to h, i.e. $M_h = \{[\sigma_h]\}$, where $\sigma_h : \langle h\rangle \to G_h$. This induces a canonical map $\phi : M \to \prod_{h\in H} M_h$. By lemma 3.10 M_h is a principal homogeneous space over $H^1(\langle h\rangle, A)$, so ϕ is a morphism of principal homogeneous spaces. Hence this induces a morphism

$$\rho = \rho_A : H^1(H, A) \to \prod_{h\in H} H^1(\langle h\rangle, A).$$

Lemma 3.11. *Let H, A and ρ_A be as above. The homomorphism ρ_A is injective for all finite H-modules A if and only if every p-Sylow subgroup H_p of H is cyclic.*

Proof. "⇒" Let $n = |H|$ and choose A to be the augmentation ideal of the group ring $\mathbf{Z}/n[H]$, i.e. A is the kernel of the map from $\mathbf{Z}/n[H]$ to $\mathbf{Z}/n$. Obviously A is a finite H-module.

Notice that we have the following exact sequence

$$0 \to A \xrightarrow{\iota} \mathbf{Z}/n[H] \xrightarrow{f} \mathbf{Z}/n \to 0,$$

where $A,\ \mathbf{Z}/n,\ \mathbf{Z}/n[H]$ are G-modules, so in particular H-modules. This gives the long exact sequence:

$$\begin{array}{ccccccccc} 0 & \to & H^0(\langle h\rangle, A) & \xrightarrow{\iota_0} & H^0(\langle h\rangle, \mathbf{Z}/n[H]) & \xrightarrow{f_0} & H^0(\langle h\rangle, \mathbf{Z}/n) & \xrightarrow{\delta_1} & \\ & & H^1(\langle h\rangle, A) & \xrightarrow{\iota_1} & H^1(\langle h\rangle, \mathbf{Z}/n[H]) & \xrightarrow{f_1} & H^1(\langle h\rangle, \mathbf{Z}/n) & & \end{array}$$

Notice that $\langle h\rangle$ acts trivially on $\mathbf{Z}$, so $H^0(\langle h\rangle, \mathbf{Z}/n) = \mathbf{Z}/n$. Furthermore

$$\mathbf{Z}/n[H] \cong \bigoplus_{i=1}^{[H:\langle h\rangle]} \mathbf{Z}/n[\langle h\rangle],$$

which gives us the identity

$$H^1(\langle h\rangle, \mathbf{Z}/n[H]) \cong \bigoplus_{i=1}^{[H:\langle h\rangle]} H^1(\langle h\rangle, \mathbf{Z}/n[\langle h\rangle]).$$

The group ring $\mathbf{Z}/n[\langle h\rangle]$ is obviously an induced $\langle h\rangle$-module, so by lemma 3.8 we have $H^1(\langle h\rangle, \mathbf{Z}/n[\langle h\rangle]) = 0$. Together this gives us that $H^1(\langle h\rangle, \mathbf{Z}/n[H]) = 0$; hence δ_1 is surjective. This means that $H^1(\langle h\rangle, A) \cong H^0(\langle h\rangle, \mathbf{Z}/n)/\ker(\delta_1)$.

To determine the kernel of δ_1 we can look at the image of f_0 under maps in the long exact sequence. The elements of $H^0(\langle h\rangle, \mathbf{Z}/n[H])$ are elements of the form $\sum_{g\in H} a_g g$, which are invariant under $\langle h\rangle$. Hence we have $a_g = a_{gh^i}$ for all $h^i \in \langle h\rangle$, so the image of f_0 is $n_h\mathbf{Z}/n$, where $n_h = |\langle h\rangle|$. This gives $\mathrm{im}(g_0) = n_h\mathbf{Z}/n$ and hence $H^1(\langle h\rangle, A) \cong (\mathbf{Z}/n)/(n_h\mathbf{Z}/n) = \mathbf{Z}/n_h$.

By assumption ρ is injective and induces the map $\mathbf{Z}/n \to \prod_{h\in H} \mathbf{Z}/n_h$, which also has to be injective, so $n = \mathrm{lcm}(n_h)_{h\in H}$. Now let us choose for each prime p precisely one arbitrary Sylow subgroup H_p. Because for a prime p all p-Sylow-subgroups are isomorphic, so $|H_p|$ is independent of our choice and $n = \prod_p |H_p|$. This means that for every p, there is one h such that $|H_p| = n_h$ and $H_p = \langle h\rangle$.

Thus H_p is cyclic, so all p-Sylow-subgroups are cyclic.

"$\Leftarrow$" Let $x \in \ker \rho$, then $\rho(x) = (x_h)_{h\in H} = (1)_{h\in H}$, so $x_h = \mathrm{Res}_{\langle h\rangle} x = 1$. Moreover by lemma 3.4 we see $\mathrm{Cor} \circ \mathrm{Res}(x) = [H : \langle h\rangle] \cdot x = 1$, so x is $[H : \langle h\rangle]$-torsion in $H^1(H, A)$ for all $h \in H$. Because all p-Sylow-subgroups H_p of H are cyclic, either H is already a p-Sylow subgroup for some prime p or x is $[H : \langle h\rangle]$-torsion for all p-Sylow-subgroups H_p. In the first case we have $H = \langle h\rangle$ so x is 1-torsion, and hence x is trivial. And in the second case x is a $\gcd([H : \langle h\rangle])_{h\in H}$-torsion. Since $n = \prod_{i=1}^{m} p_i^{k_i}$ and the index of a p_i-Sylow-subgroups is $n/p_i^{k_i}$ we get the $\gcd(n/p_i^{k_i})_{i=1}^{m} = 1$, thus x is 1-torsion. Hence ρ is injective. □

Lemma 3.12. *Let H, A, G and ρ be as above. If the homomorphism ρ is not injective, then there are two cuts $\sigma_1, \sigma_2 : H \to G$ such that*

(i) $[\sigma_1] \neq [\sigma_2]$*;*

(ii) $[\sigma_1]_h = [\sigma_2]_h \quad \forall h \in H$*;*

(iii) $\sigma_1(H)$ *and* $\sigma_2(H)$ *are Gassmann equivalent.*

Proof. The homomorphism ρ is not injective, so we can take a nontrivial element $x \in \ker \rho$. Now take an arbitrary equivalence class $[\sigma_1] \in M$. Let the other equivalence class be defined by $[\sigma_2] := {}^{x}[\sigma_1]$.

"(i)": As we saw before this action is faithful; also x is nontrivial, $[\sigma_1] \neq [\sigma_2]$.

"(ii)": Because $\rho(x) = 1$, we have for all $h \in H$, $\mathrm{Res}_{\langle h\rangle} x = x_h = 1$. Hence we have the following situation in M_h

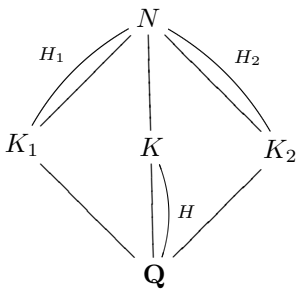
$$[\sigma_2]_h = {}^{x_h}[\sigma_1]_h = [\sigma_1]_h \quad \forall h \in H.$$

(iii) Define $H_1 = \sigma_1(H)$ and define $H_2 = \sigma_2(H)$. If for some conjugacy class c^G; $H_1 \cap c^G = \emptyset = H_2 \cap c^G$, then these sets are equal. Now assume there is an element $h \in H$ such that $\sigma_1(h) \in (H_1 \cap c^G)$ (if this set is empty, exchange the roles of H_1 and H_2). Now

$$(\sigma_2 \circ j)(\sigma_1(h)) = \sigma_2 \circ (j \circ \sigma_1)(h) = \sigma_2(h) \in H_2.$$

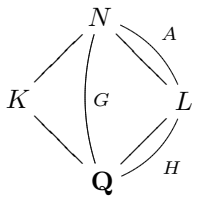
By (ii) we see that for each $h \in H$ there exists an $a \in A$ such that $\sigma_2(h) = a\sigma_1(h)a^{-1}$. Now because we already had shown that $\sigma_1(h) \in c^G$ and $a \in A$ which is a subgroup of G, we see $\sigma_2(h) \in c^G$. Hence $\sigma_2 \circ j : c^G \cap H_1 \to c^G \cap H_2$ is a well-defined map with two-sided inverse $\sigma_1 \circ j$. Therefore it is a bijection, which gives us $|c^G \cap H_1| = |c^G \cap H_2|$. So H_1 and H_2 are Gassmann equivalent. □

Remark 3.13. *We can translate the previous statements back to fields. By lemma 3.12 there exist a σ_1, σ_2 and $H_1 = \sigma_1(H)$, $H_2 = \sigma_2(H)$, with fixed fields K_1 and K_2. Because H_1 and H_2 are Gassmann equivalent by the same lemma they induce the same Dedekind zeta function. But because H_1 and H_2 are not conjugate, they are not isomorphic.*



Example

In this paragraph we want to construct an example of a field K which has a non-isomorphic field L with the same Dedekind zeta function. Let θ be the real eighth root of α, i.e. a real root of the irreducible polynomial $X^8 - \alpha \in \mathbf{Q}[X]$. Let us for example take $\alpha = 3$. Now define $K = \mathbf{Q}[\theta]$ and $L = \mathbf{Q}[\zeta_8]$ $\big(= \mathbf{Q}[i, \sqrt{2}]\big)$, where ζ_8 is an eight root of unity. The number field $N = K \cdot L$ is Galois because L is Galois. Denote the respective Galois groups by $A = \mathrm{Gal}(N/L)$, $H = \mathrm{Gal}(L/\mathbf{Q})$ and $G = \mathrm{Gal}(N/\mathbf{Q})$.



The map sending $a \in A$ to $a(\theta)/\theta$ gives an isomorphism between A and the group of eight roots of unity μ_8. Furthermore, $L \cap K = \mathbf{Q}$ and hence each element in A is determined by a unit in L, so the map $\mathrm{Gal}(N/K) \to H$; $\sigma \mapsto \sigma|_L$ has a unique inverse. Hence we get $H \cong \mathrm{Gal}(N/K) \cong \mathrm{Aut}(\mu_8)$. This gives us that G is a split extension of A by H, i.e. $G \cong A \rtimes H$.

For the construction from the previous paragraph we need a nontrivial element in the kernel of the map ρ_A. The fixed field $L^{\langle h \rangle}$ for $h \in H$ is either $\mathbf{Q}[i], \mathbf{Q}[\sqrt{2}], \mathbf{Q}[i\sqrt{2}]$ or $\mathbf{Q}[i, \sqrt{2}]$.

We claim that the map $\chi : H \to A$ given by $\chi(g) = \sqrt{2}^{\,g}/\sqrt{2}$, is an element of a nonzero class $x \in H^1(H, A)$. χ the nontrivial element we desire. When we restrict this map χ to $\langle h \rangle$ it becomes a coboundary. Define the following maps, $h_1 : \zeta_8 \mapsto \zeta_8^3$, $h_2 : \zeta_8 \mapsto \zeta_8^5$, and $h_3 : \zeta_8 \mapsto \zeta_8^7$, now

$$H \cong \mathrm{Aut}(\mu_8) = \{\mathrm{Id}, h_1, h_2, h_3\} \cong \mathbf{Z}/2 \times \mathbf{Z}/2.$$

Consider the group A; we get $\chi(\mathrm{Id}) = 1$ and $\chi(h_3) = (\zeta_8^{-1} + \zeta_8)^{h_3}/\sqrt{2} = 1$. Also

$$\chi(h_1) = (\zeta_8^3 + \zeta_8^{-3})/\sqrt{2} = -\sqrt{2}/\sqrt{2} = -1$$

and similarly $\chi(h_2) = -1$. Hence $\chi|_{\mathrm{Id}} = \chi|_{\langle h_3 \rangle} = 1$, and

$$\chi|_{\langle h_1 \rangle}(a) = i^a/i = \chi|_{\langle h_2 \rangle}(a),$$

which are coboundaries. Hence χ is a nontrivial element of the kernel of ρ.

This gives us the map $\tau := \chi \cdot \sigma$ for an arbitrary $\sigma : H \to \mathrm{Gal}(N/K)$. The fixed field of $\sigma(H)$ is by definition $K = \mathbf{Q}[\theta]$. For the fixed field of $\tau(H)$ we look at the action of an arbitrary $h \in H$, which is defined by by $h(\zeta_8) = \zeta_8^j$ for some odd $j \in \mathbf{Z}$. Then

$$\begin{aligned}
(\sqrt{2}\theta)^{\tau(h)} &= \chi(h)\sqrt{2}^{\sigma(h)}\theta^{\sigma(h)} \\
&= \frac{\zeta_8^j + \zeta_8^{-j}}{\zeta_8 + \zeta_8^{-1}}(\zeta_8^j + \zeta_8^{-j})\theta \\
&= \frac{(\zeta_8^j + \zeta_8^{-j})^2}{\sqrt{2}}\theta \\
&= \frac{\pm(\sqrt{2})^2}{\sqrt{2}}\theta \\
&= \sqrt{2}\theta.
\end{aligned}$$

Therefore, the fixed field of $\tau(H)$ is $\mathbf{Q}[\sqrt{2}\theta] = \mathbf{Q}[16\alpha]^{1/8}$. By remark 3.13, the fixed fields of $\sigma(H)$ and $\tau(H)$ are non-isomorphic and arithmetically equivalent.

3.3 Construction by permutation groups

The group G might be a subgroup of the symmetric group. Because S_l and A_l are not always split group extensions of an abelian group this is another case we would like to discuss. For the symmetric group we also want to construct arithmetically equivalent fields.

Theorem 3.14. *Let G be a subgroup of a symmetric group S_l and let H_1 and H_2 be subgroups of G. Then H_1 and H_2 are arithmetically equivalent if and only if for each $j \in \mathbf{Z}$ the number of elements in H_1 of order j is equal to the number of elements in H_2 of order j*

Proof. "$\Rightarrow$": Let T_j be the set of representatives $g \in G$ of the conjugates of order j. Let $J := \{g \in G \text{ of order } j\} = \dot{\bigcup}_{g \in T_j} g^G$. Hence

$$|J \cap H_1| = \sum_{g \in T_j} |g^G \cap H_1| = \sum_{g \in T_j} |g^G \cap H_2| = |J \cap H_2|.$$

"$\Leftarrow$" : We have a H_1 and H_2 such that the condition is satisfied. This gives us an embedding in S_l, where $l = |H_1| = |H_2|$. Now take two arbitrary elements $h, h' \in H_1 \cup H_2$. Assume that $h \in H_1$ (otherwise just switch H_1 and H_2). Now h acts on H_1 with left multiplication, so by the embedding into S_l, h is a product of l/j cycles of length j, where j is the order of h. By similar argumentation the same is true for h', so h and h' have equal cycle structure and hence are conjugates in S_l.

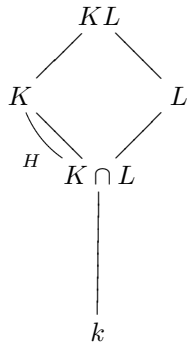
If both H_i have $H_i \cap c^G = \emptyset$ then they are equal. So assume that we have an element of $h_1 \in H_1 \cap c^G$, now by assumption there exists an element $h_2 \in H_2$ of the same order, so these elements are conjugate by embedding into S_l. Hence $h_2 \in H_2 \cap c^G$ and we get

$$\begin{aligned} |H_1 \cap c^G| &= |\{h \in H_1 \mid \text{order}(h) = \text{order}(c)\}| \\ &= |\{h \in H_2 \mid \text{order}(h) = \text{order}(c)\}| \\ &= |H_2 \cap c^G|. \end{aligned}$$

□

4 Arithmetic equivalent number field extensions

Extensions of two arithmetically equivalent number fields may be arithmetically equivalent.



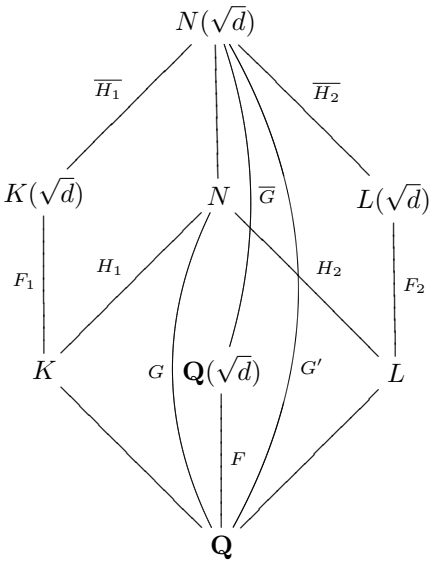
In this chapter we develop some conditions for this extensions to be arithmetically equivalent this is the case. First we recall a standard theorem of algebra.

Theorem 4.1. (c.f. [Lan02]) *Let k be an arbitrary field and let K and L be two finite field extension of k. Furthermore let K be a Galois extension of k and let KL be a Galois extension of L, with Galois group G. Then K is Galois over $K \cap L$ with Galois group H, and $H \cong G$.*

Proof. We can define the restriction map $\rho : G \to H$; $g \mapsto g|_K$. The image of this restriction are the automorphism of K, with fixed field $K \cap L$, so this map is well-defined. By definition ρ is an homomorphism. This map is injective, because an arbitrary element of KL can be written as a linear continuation of elements of K and L. If $g|_K = \mathrm{Id}_K$ acts as the identity on K and on L, and hence $g = \mathrm{Id}_{KL}$, so indeed ρ is injective. Furthermore we have $[K : K \cap L] = [KL : L]$, so $|G| = |H|$, and hence ρ is an isomorphism. □

4.1 Quadratic extensions

As before, we look at the number fields K, and L and an arbitrary finite Galois extension N of these fields. We look at the quadratic extension $X^2 - d$ of K and L, where d is some integer. Now the number field $N(\sqrt{d})$ is again Galois over both $K(\sqrt{d})$ and $L(\sqrt{d})$. The situation is sketched in the diagram on the right-hand-side of this page.



We want to distinguish the different situations whether we really have quadratic extensions or not. Note that if either K or L contains $\sqrt{d}$, but $K \cap L$ does not. Then one extension is the original field K or L and the other extension is a quadratic extension $K(\sqrt{d})$ or $L(\sqrt{d})$. If K and L are arithmetically equivalent then the degree of these extensions is equal. But then $K(\sqrt{d})$ and $L(\sqrt{d})$ do not have an equal degree over $\mathbf{Q}$, so by theorem 2.11 they are not arithmetically equivalent. Similarly, if $K(\sqrt{d})$ and $L(\sqrt{d})$ are arithmetically equivalent, then K and L are not arithmetically equivalent.

Now we can look at the more interesting case where $\sqrt{d}$ is neither an element of K or L:

Theorem 4.2. *Let K and L be two number fields. Let N be Galois over $\mathbf{Q}$ containing K and L, and let $d \in \mathbf{Z}$. Let $\sqrt{d}$ be neither an element of K or L:*

> *K and L are arithmetically equivalent if and only if $K(\sqrt{d})$ and $L(\sqrt{d})$ are arithmetically equivalent.*

Proof. First let $\sqrt{d} \notin N$, thus $\sqrt{d}$ is not an element of K or L. Now $N(\sqrt{d}), K(\sqrt{d})$ and $L(\sqrt{d})$ are genuine quadratic extensions of N, K and L. Notice that

$$N \cap K(\sqrt{d}) = K, \text{ and } \quad K(\sqrt{d}) \cdot N = N(\sqrt{d}),$$

and N/K is Galois with Galois group H_1, so by theorem 4.1 this gives a natural isomorphism between H_1 and $\overline{H_1} = \mathrm{Gal}(N(\sqrt{d})/K(\sqrt{d}))$. Similarly, we get a natural isomorphism between $H_2 = \mathrm{Gal}(N/L)$ and $\overline{H_2} = \mathrm{Gal}(N(\sqrt{d})/L(\sqrt{d}))$ and between $G = \mathrm{Gal}(N/\mathbf{Q})$ and $\overline{G} = \mathrm{Gal}(N(\sqrt{d}/\mathbf{Q}(\sqrt{d}))$. By these isomorphisms we get the equality $|H_i \cap c^G| = |\overline{H_i} \cap c^{\overline{G}}|$ for $i = 1, 2$. Let $G' = \mathrm{Gal}(N(\sqrt{d})/\mathbf{Q})$. Now if $c \in G' \backslash \overline{G}$, i.e. c is the map which sends $\sqrt{d}$ to $-\sqrt{d}$ and fixes $\mathbf{Q}$, then the conjugates of c act the same on $\mathbf{Q}(\sqrt{d})$ and hence $\overline{H_i} \cap c^{G'} = \emptyset$. The group G' is actually the direct product of the two subgroups, i.e. $G' = \overline{G} \times F$, where the subgroup $F = \mathrm{Gal}(\mathbf{Q}(\sqrt{d})/\mathbf{Q})$ consists of the identity and the element c.

If we take the conjugation of $c \in \overline{G} \times \{1\}$ by an element $g \in G'$ which we can write as a product $\bar{g}f \in \overline{G} \times F = G'$, then we get $gcg^{-1} = \bar{g}fcf^{-1}\bar{g}^{-1} = \bar{g}c\bar{g}^{-1}$. If we assume $c \in \overline{G} \times \{1\}$, we get the following equality

$$\overline{H_i} \cap c^{G'} = \{h \in \overline{H_i} \mid \exists g = \bar{g}f \in G' \ ; \ h = \bar{g}c\bar{g}^{-1}\} = 2 \cdot (\overline{H_i} \cap c^{\overline{G}}).$$

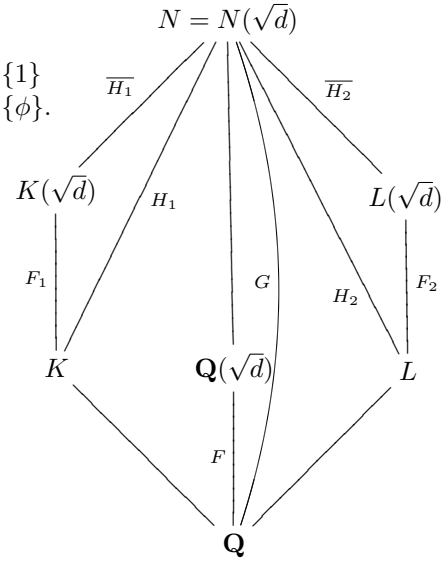
Hence

$$|\overline{H_i} \cap c^{G'}| = \begin{cases} 2 \cdot |\overline{H_i} \cap c^{\overline{G}}| & \text{if } c \in \overline{G} \times \{1\} \\ 0 & \text{if } c \in \overline{G} \times \{\phi\}. \end{cases}$$

Therefore, H_1 and H_2 are Gassmann equivalent if and only if

$$|\overline{H_1} \cap c^{G'}| = |\overline{H_2} \cap c^{G'}|.$$

Finally, we have the case where $\sqrt{d} \in N$, but $\sqrt{d}$ is not an element of either K or L. In this case $K(\sqrt{d})$ and $L(\sqrt{d})$ are both quadratic extensions. Now the diagram collapses and we are in the situation of the diagram on our right-hand-site.



Because the extension $\mathbf{Q}(\sqrt{d})$ over $\mathbf{Q}$ is Galois, $K \cap \mathbf{Q}(\sqrt{d}) = \mathbf{Q}$ and

$$K \cdot \mathbf{Q}(\sqrt{d}) = K(\sqrt{d}),$$

we get by theorem 4.1 $F \cong F_1 = \mathrm{Gal}(K(\sqrt{d})/K)$ and similarly, $F \cong F_2 = \mathrm{Gal}(L(\sqrt{d})/L)$. Thus, H_i is actually the direct product $H_i = \overline{H_i} \times F_i \cong \overline{H_i} \times F$. Therefore,

$$\begin{aligned} |H_i \cap c^G| &= |\overline{H_i} \times \{1\} \cap c^G| + |\overline{H_i} \times \{\phi\} \cap c^G| \\ &= |\{h \in \overline{H_i} \times \{1\} \mid \exists g \in G; h = c^g\}| \\ &\quad + |\{h \in \overline{H_i} \times \{\phi\} \mid \exists g \in G : h = c^g\}| \\ &= \begin{cases} |\overline{H_i} \cap c^G| + 0 & \text{if} \quad c \in F \times \{1\} \\ 0 + |\overline{H_i} \cap c^G| & \text{if} \quad c \in F \times \{\phi\} \end{cases} \\ &= |\overline{H_i} \cap c^G|. \end{aligned}$$

□

An almost similar result was already given by Jangheon Oh in [Oh98]. He showed in this article that if two quadratic extensions of number fields are arithmetically equivalent, then the number fields them selfs are arithmetically equivalent.

4.2 Galois extensions

We want to generalize the theory about quadratic extensions in the last paragraph to the more general case of Galois extensions. As before, let K and L be two number fields. Assume we have a number field M which is Galois over $\mathbf{Q}$, with an abelian Galois group. Define $N := KLM$, which is Galois over $\mathbf{Q}$, and an extension of K, L and M. Let us assume that $K \cap M$ and $L \cap M$ are Galois extensions over $\mathbf{Q}$ of equal degree.

Notice that by the Kronecker-Weber theorem (c.f. [Neu92], [Ste02]) M is an abelian Galois extension of $\mathbf{Q}$ if and only if it is a subfield of a cyclotomic field, i.e. a field obtained by adjoining a root of unity to $\mathbf{Q}$. In particular the quadratic number fields are subfields of cyclotomic fields, so $M = \mathbf{Q}[\sqrt{d}]$ is a special case of this situation. Now we can formulate the following theorem in the same way as our previous theorem:

Theorem 4.3. *Let K and L be two number fields. Let M be a number field, which is abelian Galois over $\mathbf{Q}$, such that both $K \cap M$ and $L \cap M$ are Galois over $\mathbf{Q}$ and have the same degree. Then we have*
The number fields K and L are arithmetically equivalent if and only if the number fields KM and LM are arithmetically equivalent.

Proof. Because M is Galois over $\mathbf{Q}$, we have KM is Galois over K. Denote the Galois group of KM over K by F_1. The diagram of K, M, the intersection $K \cap M$ and the product KM gives by theorem 4.1 $F_1 \cong \mathrm{Gal}(M/(K \cap M))$.

By assumption $K \cap M$ and $L \cap M$ are Galois over $\mathbf{Q}$, so they are Galois over $K \cap L \cap M$, with Galois groups G_1 respectively G_2. Define the Galois groups $G_1 = \mathrm{Gal}((K \cap M)/(K \cap L \cap M))$ and $G_2 = \mathrm{Gal}((L \cap M)/(K \cap L \cap M))$.

As we can see in the above diagram that $(K \cap M)(L \cap M) = KL \cap M$ gives by theorem 4.1 $G_1 \cong \overline{G_1}$, where $\overline{G_1}$ is defined as $\mathrm{Gal}((KL \cap M)/(L \cap M))$. Similarly $G_2 \cong \overline{G_2}$, where $\overline{G_2}$ is the Galois group of $KL \cap M$ over $K \cap M$. Because M is Galois over $\mathbf{Q}$, M is Galois over $KL \cap M$. Combining all this, we obtain

$$F_1 \cong \mathrm{Gal}(M/(K \cap M)) = \mathrm{Gal}(M/(KL \cap M)) \times \overline{G_2} \cong \mathrm{Gal}(M/(KL \cap M)) \times G_2.$$

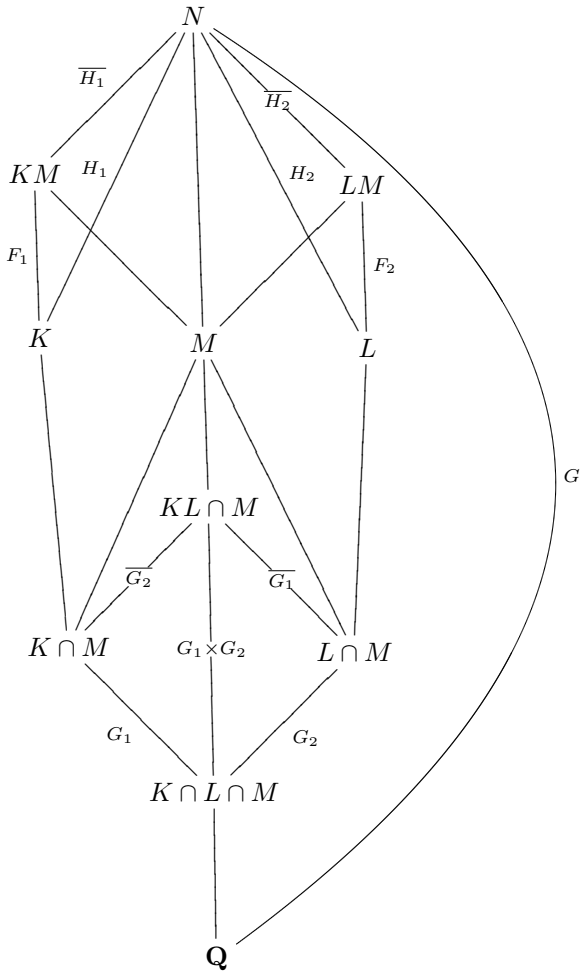
Similarly, let F_2 be the Galois group of LM over L. We get as before

$$F_2 \cong \mathrm{Gal}(M/(L \cap M)) = \mathrm{Gal}(M/(KL \cap M)) \times \overline{G_1} \cong \mathrm{Gal}(M/(KL \cap M)) \times \ G_1.$$

Let G define the Galois group of N over $\mathbf{Q}$. Furthermore $K \cap L \cap M$ is Galois over $\mathbf{Q}$, and N is Galois over M, so

$$\begin{aligned} G &= \mathrm{Gal}(N/M) \times \mathrm{Gal}(M/(KL \cap M) \times G_1 \times G_2 \times \mathrm{Gal}((K \cap L \cap M)/\mathbf{Q}) \\ &= \mathrm{Gal}(N/M) \times G_i \times F_i, \end{aligned}$$

for $i \in \{1, 2\}$.



Let $H_1 = \mathrm{Gal}(N/K)$, $H_2 = \mathrm{Gal}(N/L)$, $\overline{H_1} = \mathrm{Gal}(N/KM)$ and $\overline{H_2} = \mathrm{Gal}(N/LM)$. Let $i \in \{1, 2\}$, let ϕ be an element of F_i. Now we can consider the case where the part on F_i of $c \in G$ is equal to the map ϕ. The conjugations of c give in the part of F_i conjugations of ϕ. The group F_i is isomorphic to a subgroup of the Galois group of M over $\mathbf{Q}$, so F_i is abelian. Hence the conjugations of ϕ are just ϕ itself, which gives us the following equality

$$\begin{aligned} |H_i \cap c^G| &= |(\overline{H_i} \times F_i) \cap c^G| \\ &= \sum_{\phi \in F_i} |(\overline{H_i} \times \{\phi\}) \cap c^G| \\ &= |\overline{H_i} \cap c^G|. \end{aligned}$$

By theorem 2 two fields are arithmetically equivalent if and only if their corresponding Galois groups are Gassmann equivalent. Hence K and L are arithmetically equivalent if and only if $|H_1 \cap c^G| = |H_2 \cap c^G|$ for all $c \in G$. By the previous equation this is true if and only if $|\overline{H_1} \cap c^G| = |\overline{H_2} \cap c^G|$ for all $c \in G$, which is equivalent with the case that KM and LM are arithmetically equivalent. $\square$

5 L-series

The zeta function and the Artin L-series are closely related. We start by defining representations, which the Artin character defines in a natural way. We consider these characters because they are defined in a more group theoretically way. We define the Artin L-series, and look at the relation between the more general Dedekind zeta function and this L-series.

5.1 Representations and Artin Characters

In this paragraph we start by defining a representation and giving some elementary properties of such a representation. Secondly, we describe how to define an Artin character by a representation. Finally, we give a theorem which states that the Dedekind zeta function of a quadratic extension is the product of the Dedekind zeta function of the underlying number field and the Artin L-series of the associated quadratic character. By the previous chapter about extensions of number fields, we know that if two number fields are arithmetically equivalent, then the quadratic extensions are also arithmetically equivalent. Hence we have equal Artin L-series.

Let K be a number field and L be a finite extension of L, let $\mathfrak{p}$ be a prime of K and $\mathfrak{P}$ a prime of L which lies above $\mathfrak{p}$. Let us first briefly recall the definition of the Frobenius automorphism. For more detail on this subject we refer to the literature, for example [Ros02], [Neu92], [Lan02], [CF67a].

Definition 5.1. *The* Frobenius automorphism $(\mathfrak{P}, L/K)$ *for* $\mathfrak{P}$ *is the automorphism of* L *such that*

$$(\mathfrak{P}, L/K)(a) \equiv a^q \mod \mathfrak{P},$$

for all $a \in \mathcal{O}_L$ *(ring of integers), where* q *is the number of elements in the residue class field* $\mathcal{O}_K/\mathfrak{p}$ *of* $\mathfrak{p}$.

For a subgroup A of G the G-module V^A is the submodule of V on which the group A acts trivially. Because $G_{\mathfrak{P}}/I_{\mathfrak{P}}$ is isomorphic to $\mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$, we have that $G_{\mathfrak{P}}/I_{\mathfrak{P}}$ is generated by the Frobenius automorphism $(\mathfrak{P}, L/K)$. Note that our representation does not have to be faithful (injective as homomorphism), as $I_{\mathfrak{P}}$ is in the kernel. But the Frobenius automorphism is an endomorphism of the G-module $V^{I_{\mathfrak{P}}}$.

Now let us define a representation and some properties:

Definition 5.2. *A* representation (ρ, V) *of a Galois group* G *is an action of* G *on a finite-dimensional* $\mathbf{C}$*-vector space* V*, or equivalently a homomorphism*

$$\rho : G \to GL(V).$$

The characteristic polynomial *of a representation* (ρ, V) *is the polynomial*

$$\det(1 - (\mathfrak{P}, L/K)t; V^{I_{\mathfrak{P}}}),$$

where this is the determinant of the map $1 - (\mathfrak{P}, L/K)_{\mathfrak{P}}t$*, written as matrix with the basis of* $V^{I_{\mathfrak{P}}}$*. The* degree *of a representation* (ρ, V) *of* G *is the dimension of* V*. Two representations* (ρ, V) *and* (ρ', V') *are called* equivalent *if the modules* V *and* V' *are* G*-isomorphic. A representation is called* irreducible *if the* G*-module* V

does not have any proper subspace. The trivial representation $\rho : G \to GL(V)$ *is the representation defined by* $dim(V) = 1$ *and* $\rho(\sigma) = 1$ *for all* $\sigma \in G$. *The* regular representation *is the representation with the group ring* $\mathbf{C}[G]$ *as associated vector space.*

Every representation factors into a direct sum of irreducible representations, i.e. $V = \bigoplus_{i=1}^{s} V_i$. Hence a representation ρ is equivalent to the sum of the irreducible representations ρ_α with a certain multiplicity, i.e. $\rho \sim \sum_\alpha r_\alpha \rho_\alpha$, with $r_\alpha \in \mathbf{Z}$.

Let (ρ, V) be a representation of a subgroup H of G. This representation induces a representation $\left(\text{ind}(\rho), \text{Ind}_G^H(V)\right)$ of the group G, where

$$\text{Ind}_G^H(V) = \{f : G \to V \mid \forall \tau \in H; f(\tau x) = \tau f(x)\}.$$

Definition 5.3. *The* character *of the representation* ρ *the map* $\chi_\rho : G \to \mathbf{C}$ *with* $\chi_\rho(\sigma)$ *is the trace of the multiplication matrix of* $\rho\sigma$.
A character is called irreducible *if it is associated to an irreducible representation. The* trivial character *is the character associated to the trivial representation, and is denoted by* $\mathbf{1}$. *Furthermore the character associated with the regular representation* $\mathbf{C}[G]$ *is called the* regular character *and denoted by* r_G. *This character can be written as the sum over all irreducible characters of* G: $r_G = \sum_{\chi^{irr.}} \chi(1)\chi$.

Two representations are equivalent if and only if the associated characters are equal: Assume (ρ, V) and (ρ', V') are equivalent, then there is a G-isomorphism $f : V \to V'$. Hence $\rho' = f\rho f^{-1}$, so $\chi_{\rho'} = \chi_{f\rho f^{-1}} = \chi_f \chi_\rho \chi_{f^{-1}} = \chi_\rho$. Hence the representations are equivalent.

A representation $\rho \sim \sum_\alpha r_\alpha \rho_\alpha$ with the sum over all irreducible characters, has that the associated character χ_ρ is equal to the sum $\sum_\alpha r_\alpha \chi_{\rho_\alpha}$.

5.2 Artin L-series

Let K be a number field and let L be a finite extension Galois over $\mathbf{Q}$. Let $\mathfrak{p}$ be a prime of K and $\mathfrak{P}$ be a prime of L which lies above $\mathfrak{p}$. Now we can define the Artin L-series:

Definition 5.4. *The* Artin L-series *is a function of the form*

$$\mathcal{L}(L/K, \chi, s) = \prod_{\mathfrak{p}} \det(1 - \rho((\mathfrak{P}, L/K))\mathcal{N}(\mathfrak{p})^{-s}; V^{I_\mathfrak{P}})^{-1},$$

where ρ *is the associated representation of the character* χ.

Notice that we have the following fact about Artin L-series:

Remark 5.5. *Note that the Artin L-series of the trivial character is equal to the Dedekind zeta function, by the following equality*

$$\mathcal{L}(L/K, \mathbf{1}, s) = \prod_{\mathfrak{p}} \det(1 - \mathcal{N}(\mathfrak{p})^{-s}; V^{I_\mathfrak{P}})^{-1} = \zeta_K(s),$$

where $\mathbf{1}$ *denotes the trivial character.*

Lemma 5.6. *Let* K *be a number field and let* L *be a finite extension of* K. *If* χ *and* χ' *are two characters associated to representations of* $Gal(L/K)$, *then*

$$\mathcal{L}(L/K, \chi + \chi', s) = \mathcal{L}(L/K, \chi, s)\mathcal{L}(L/K, \chi, s).$$

Proof. Let (ρ, V) and (ρ', V') be representations of the Galois group $\mathrm{Gal}(L/K)$, with associated to the characters χ, and χ'. The direct sum of these representations, $(\rho \oplus \rho', V \oplus V')$, is a representation of the character χ''

$$\chi''(\sigma) = \mathrm{tr}(\rho(\sigma) + \rho'(\sigma)) = \mathrm{tr}(\rho(\sigma)) + \mathrm{tr}(\rho'(\sigma)) = \chi(\sigma) + \chi'(\sigma).$$

Notate $\phi_{\mathfrak{P}} = (\mathfrak{P}, L/K)$, then,

$$\det(1 - \rho(\phi_{\mathfrak{P}})t; (V \oplus V')^{I_{\mathfrak{P}}}) = \det(1 - \rho(\phi_{\mathfrak{P}})t; V^{I_{\mathfrak{P}}}) \det(1 - \rho'(\phi_{\mathfrak{P}})t; V'^{I_{\mathfrak{P}}}).$$

□

Let us now state a theorem which give a formula for the zeta function of a quadratic extension in terms of the Artin L-series:

Theorem 5.7. *Let K be a number field and let χ_d be the quadratic character associated to $\sqrt{d}$. Then*

$$\zeta_{K(\sqrt{d})}(s) = \zeta_K(s)\mathcal{L}(L/K, \chi_d, s).$$

Proof. By remark 5.5 we have that $\zeta_{K(\sqrt{d})}(s) = \mathcal{L}(K(\sqrt{d})/K(\sqrt{d}), \mathbf{1}, s)$. Let σ be an automorphism of $K(\sqrt{d})$, such that $\sigma(\sqrt{d}) = -\sqrt{d}$ an which is the identity on K. The Galois group of the extension $K(\sqrt{d})$ of K is $G = \{1, \sigma\}$, so the irreducible characters of this Galois group are the trivial character and the quadratic character. Let $\mathfrak{p}$ be a prime of K and let $\mathfrak{P}$ be a prime of $K(\sqrt{d})$ which lies above $\mathfrak{p}$. The decomposition group $G_{\mathfrak{P}}$ is a subgroup of G, so is either equal to G or trivial, depending on the splitting type of $\mathfrak{p}$. The inertia group $I_{\mathfrak{P}}$ is a subgroup of this decomposition group. Both the form of the inertia group and the decomposition group depends on how the prime $\mathfrak{p}$ splits. We can see that there are three different ways of a prime $\mathfrak{p} \subset K$ to split in $K(\sqrt{d})$. The prime can be inert, it can be ramified or it can be splits. Let (ρ, V) be the representation of our group G and let (ρ', W) be the representation of the subgroup H. We claim that in all three cases $\det(1 - (\mathfrak{P}, K(\sqrt{d})/K)t; V) = \det(1 - (\mathfrak{P}, K(\sqrt{d}/K)^f t^f; W)^{n/f}$, where f is the inertia degree of $\mathfrak{P}$ over $\mathfrak{p}$, e is the ramification index and n is the degree of the extension.

First, consider the case were the prime is inert in $K(\sqrt{d})$. Then $G_{\mathfrak{P}} = G$, $e = 1$ and $f = 2$, so $I_{\mathfrak{P}} = 1$. In this case the Frobenius automorphism $(\mathfrak{P}, K(\sqrt{d})/K)$ can be either the identity or σ. The induced representation of $(\mathfrak{P}, K(\sqrt{d})/K)$ is $V = \mathrm{Ind}_G^1(W) = \{f : G \to W\}$. Take the representatives of G, so we can write V as the direct sum $V = W \oplus \sigma W$. Now let A be the multiplication matrix of $(\mathfrak{P}, K(\sqrt{d})/K)^2$ with respect to $w_1, \ldots, w_d$, the basis of W, so A the $d \times d$-unit matrix. Then the multiplication matrix of $(\mathfrak{P}, K(\sqrt{d})/K)$ with respect to the basis $w_1, \ldots, w_d, (\mathfrak{P}, K(\sqrt{d})/K)w_1, \ldots, (\mathfrak{P}, K(\sqrt{d})/K)w_d$ of V is:

$$\begin{pmatrix} 0 & I \\ A & 0 \end{pmatrix}$$

where I is the $d \times d$-unit matrix. Because these matrices commute

$$\begin{aligned} \det(1 - (\mathfrak{P}, K(\sqrt{d})/K)t; V) &= \det \begin{pmatrix} I & -tI \\ -tI & I \end{pmatrix} \\ &= \det(II - (-tI)(-tI)) \\ &= \det(I - t^2 I; W). \end{aligned}$$

Secondly, let us consider the case where the prime $\mathfrak{p}$ splits, i.e. $\mathfrak{p} = \mathfrak{P}_1\mathfrak{P}_2$. Note $G_{\mathfrak{P}_i} = 1$, so the inertia group $I_{\mathfrak{P}} = 1$. In this case by transitivity of G on

primes above $\mathfrak{p}$, $\sigma\mathfrak{P}_1 = \mathfrak{P}_2$. Hence the group $G_{\mathfrak{P}_i}/I_{\mathfrak{P}_i}$ is trivial, so our Frobenius automorphism $(\mathfrak{P}_i, K(\sqrt{d})/K)$ are trivial. The induced representation is given by $(\mathrm{ind}(\rho), V)$, where $\mathrm{ind}(\rho)$ is a map $G \to GL(V)$, and

$$\mathrm{Ind}_G^H(W) = \{g : G \to V \mid \forall \tau \in H : g(\tau x) = \tau g(x)\}.$$

As $V = W \oplus W$; $\det(1 - (\mathfrak{P}, K(\sqrt{d})/K)t; V) = \det(1 - (\mathfrak{P}, K(\sqrt{d})/K)t; W)^2$.

Finally, consider the case where the prime $\mathfrak{p}$ ramifies, i.e. $\mathfrak{p} = \mathfrak{P}^2$. In this case we have $e = 2$ and $f = 1$, so $G_{\mathfrak{P}} = G$ and $G = I$. Let $G' = G/I = 1$ and $I' = 1$. Then

$$\mathrm{Ind}_{G'}^{H'}(W) = \{g' : G' \to W \mid \forall \tau \in I' : g'(\tau x) = \tau g'(x)\}.$$

The map g is defined from our original G to W. We have that g is invariant under I if and only if g is constant on the cosets of G mod I. This is the case if and only if g' is constant on the cosets of G' mod I'. Which is equivalent to the case that g' is invariant under I'

Hence this induced representation is equal to the original induced representation, and therefore we can consider our reduced groups without loss of generality. But then $G' = I' = 1$, so we are in the case where $W = V$ and hence we indeed have $\det(1 - (\mathfrak{P}, K(\sqrt{d})/K)t; V) = \det(1 - (\mathfrak{P}, K(\sqrt{d})/K)t; W)$.

In this way we obtain the equality $\mathcal{L}(K(\sqrt{d})/K(\sqrt{d}), \mathbf{1}, s) = \mathcal{L}(K(\sqrt{d})/K, r_G, s)$. Since the regular character of G is $r_G = \mathbf{1} + \chi_d$ we get

$$\begin{aligned}
\zeta_{K(\sqrt{d})}(s) &= \mathcal{L}(K(\sqrt{d})/K(\sqrt{d}), \mathbf{1}, s) \\
&= \mathcal{L}(K(\sqrt{d})/K, r_G, s) \\
&= \mathcal{L}(K(\sqrt{d})/K, \mathbf{1}, s) \cdot \mathcal{L}(K(\sqrt{d})/K, \chi_d, s) \\
&= \zeta_K(s) \cdot \mathcal{L}(K(\sqrt{d})/K, \chi_d, s).
\end{aligned}$$

□

Consider two arithmetically equivalent number fields K and L, i.e. inducing the same zeta function $\zeta_K(s) = \zeta_L(s)$. As before, let N be an extension of both K and L and a Galois extension of over $\mathbf{Q}$. If $\sqrt{d}$ is not an element of K or L, then the quadratic extensions are also arithmetically equivalent (theorem 4.2). Our previous theorem now yields the following equality

$$\zeta_K(s)\mathcal{L}(N/K, \chi, s) = \zeta_{K(\sqrt{d})}(s) = \zeta_{L(\sqrt{d})}(s) = \zeta_L(s)\mathcal{L}(N/L, \chi, s).$$

Combining this result together with the equality of the zeta function we get the following corollary.

Corollary 5.8. *Let L and K be arithmetically equivalent number fields, and let χ be the quadratic character associated to $\sqrt{d}$. If $\sqrt{d}$ is not in either L or K, then $\mathcal{L}(N/K, \chi, s) = \mathcal{L}(N/L, \chi, s)$.*

6 Classical zeta function over function fields

Algebraic number theory deals with finite algebraic extensions of $\mathbf{Q}$. It is to develop similar theory over function fields, most definitions in algebraic number theory have equivalent definitions in number theory over global function fields. In this chapter we first describe some basic properties of function fields, and because the definitions have a lot in common we will try to develop an analogue to Perlis' theorem over function fields. Then we shall examine the classical (Artin-Weil) zeta function, which is described in the book of M. Rosen [Ros02]. And we shall also examine the Goss zeta function.

6.1 Definitions and properties of function fields

Let us first give a definition of a function field. There are algebraic and global function fields; let us start with the more general algebraic function field:

Definition 6.1. *An* algebraic function field *over a field* $\mathbf{F}$ *is a field containing* $\mathbf{F}$ *and at least one element* t *which is transcendental over* $\mathbf{F}$*. The basic field* $\mathbf{F}$ *is called the* constant field *of our function field. And the number of independent transcendental elements which our field contains is called the* transcendence degree *over* $\mathbf{F}$*.*
A global function field *is an algebraic function field with a finite constant field, and transcendence degree one. A* prime P *of a function field* K *is the maximal ideal together with its discrete valuation ring* $\mathcal{O}_P$ *such that* $\mathbf{F} \subset \mathcal{O}_P$ *and* $\mathcal{O}_P/P = K$*.*

Most number theory carries over only to global function fields, so we will restrict ourselves to this case. Hence our function field will be always of the form $K = \mathbf{F}(t)$, where we assume $\mathbf{F}$ has $q = p^k$ elements and t is transcendental over $\mathbf{F}$.

Proposition 6.2. *A prime* P *of* $\mathbf{F}(t)$ *is either an irreducible polynomial in* $\mathbf{F}[t]$ *or it is the polynomial* $1/t$*.*

Proof. By the definition of $R = \mathcal{O}_P$, either $t \in R$ or $1/t \in R$. Suppose $t \in R$. Let $\mathbf{m}$ be the unique maximal ideal of R. Define $\mathbf{p} = \mathbf{m} \cap \mathbf{F}[t]$. Because $\mathbf{m}$ is a prime ideal this is a prime ideal of $\mathbf{F}[t]$. Hence either $\mathbf{p} = (0)$ or $\mathbf{p} = (f)$ with f an irreducible polynomial of $\mathbf{F}[t]$. Now suppose that some polynomial g of $\mathbf{F}[t]$ is not in our prime $\mathbf{p}$, then $g \notin \mathbf{m}$, so we have $1/g \in R$, and hence $R = \mathbf{F}[t]_{\mathbf{p}}$. If $\mathbf{p} = (0)$, then R is our original function field.

In the second case we have $1/t \in R$ and (to exclude the first case) $t \notin R$. Note $\mathbf{F}[1/t] \subset R$. By similar arguments as in the first case we find $R = \mathbf{F}[1/t]_{(f)}$ for an irreducible polynomial f of $\mathbf{F}$. Because $t \notin R$, so $1/t \in \mathbf{m}$, $\mathbf{p} = (1/t)$ and hence $R = \mathbf{F}[1/t]_{(1/t)}$. □

We need also some other definitions of properties of function fields:

Definition 6.3. *The associated* order *to* $\mathcal{O}_P$ *is denoted by* ord_P*. The* degree *of* P*, denoted by* $deg(P)$*, is the dimension of* $\mathcal{O}_P/P$ *over* $\mathbf{F}$*.*

The group of divisors *of* K*, denoted by* $\mathcal{D}_K$*, is the free abelian group generated by the primes, e.g.* $D = \sum_P ord_P(D)P$*, where the coefficient* $ord_P(D)$ *is an integer uniquely determined by* D*. If all coefficients are positive, then the divisor is called* effective*. We denote this by* $D \geq 0$*. The* degree *of a divisor is*

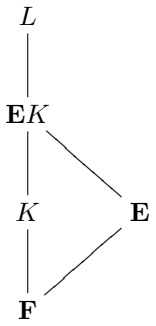
deg$(D) = \sum_P ord_P(D)\deg(P)$. *The* norm *of a divisor* D*, denoted by* $\mathcal{N}(D)$ *is equal to* $q^{\deg D}$*, where* q *is the number of elements of our finite field* $\mathbf{F}$*.*

The classical zeta function of a function field K as defined by Artin and Weil is

$$\zeta_K(s) = \sum_{A \in \mathrm{Div}(K) A \geq 0} \mathcal{N}(A)^{-s},$$

Because the divisors form a free abelian group on the set of primes

$$\zeta_K(s) = \prod_P (1 - \mathcal{N}(P)^{-s})^{-1}.$$



Let L/K be an algebraic field extension. Now the constant field $\mathbf{E}$ of L is the algebraic closure in L of the constant field $\mathbf{F}$, i.e. $\mathbf{E} = \overline{\mathbf{F}} \cap L$.

Definition 6.4. *If the constant field does not change, i.e.* $\mathbf{F} = \mathbf{E}$*, then we call the function field extension a* geometric extension*. If* $L = \mathbf{E}K$*, then we call this extension a* constant field extension*.*

Note that the extension L over $\mathbf{E}K$ is always a geometric extension and that the extension $\mathbf{E}K$ over K is always a constant field extension.

6.2 Arithmetically equivalent function fields

In this paragraph we give a counterexample of the analogue of Perlis' theorem over function fields with the classical zeta function. After this we can look into the causes of this problem over function fields. Secondly, we exam the rest of the proof of this analogue of Perlis' theorem to see what other things still work over function fields. And finally, we will try to repair the problem in Perlis' theorem.

6.2.1 Theorem of arithmetically equivalent function fields adapted

Let us first briefly recall the first part of Perlis' theorem:

Theorem 6.5. see also 2.11)
Let K *and* K' *be two number fields. The following are equivalent:*

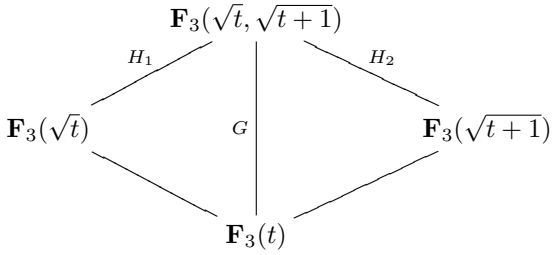
(a) $\zeta_K(s) = \zeta_{K'}(s)$*;*

(b) The number fields K *and* K' *are arithmetically equivalent;*

(c) $P_K(A) \doteq P_{K'}(A)$ *for every tuple* A*;*

(d) $H = Gal(N/K)$ *and* $H' = Gal(N/K')$ *are Gassmann equivalent.*

We give with an example of function fields which have the same zeta function, but are not Gassmann equivalent.



Let us consider the function field $\mathbf{F}_3(t)$. We have two quadratic extensions of our ground field $\mathbf{F}_3(t)$, one is the splitting field of X^2-t and the other the splitting field of $X^2-(t+1)$. The extensions have the same constant field, and therefore are these geometric extensions. The extensions are Galois (the polynomials are all separable and they are obviously normal), with Galois groups isomorphic $\mathbf{Z}/2$. Because the intersection of these field extensions is our ground field, the product of these fields $\mathbf{F}_3(\sqrt{t},\sqrt{t+1})$ has a Galois group G isomorphic to $\mathbf{Z}/2\times\mathbf{Z}/2$ (by theorem 4.1). Note that G is abelian; therefore any conjugation of an element c is just c. Let $H_1=\mathrm{Gal}\left(\mathbf{F}_3(\sqrt{t},\sqrt{t+1}/\mathbf{F}_3(\sqrt{t})\right)$ and $H_2=\mathrm{Gal}\left(\mathbf{F}_3(\sqrt{t},\sqrt{t+1}/\mathbf{F}_3(\sqrt{t})\right)$. For $i\in\{1,2\}$, $c^G\cap H_i$ is either equal to $\{c\}$ or empty depending on whether c is an element of H_i or not. But the intersection of H_1 and H_2 is equal to the identity. Let c be the non-trivial element of H_1. Then it is not an element of H_2 and hence there exist a $c\in G$ such that $|c^G\cap H_1|\neq|c^G\cap H_2|$. So H_1 and H_2 are not Gassmann equivalent. But the fields $\mathbf{F}_3(\sqrt{t})$ and $\mathbf{F}_3(\sqrt{t+1})$ are isomorphic by the map sending the element t to $t+1$. Therefore the zeta functions over both function fields are equal. Hence we cannot simply transpose Perlis' theorem to function fields for this zeta function.

Now the question arises whether the primes in these function fields still split in the same manner. For example take a prime $t-1$ in the ring of integers $\mathbf{F}_3[t]$ of $bF_3(t)$. If we look at this prime in $\mathbf{F}_3[\sqrt{t}]$, we see that this prime splits into $\sqrt{t}-1$ and $\sqrt{t}+1$. But if we consider the prime $t-1$ in $\mathbf{F}_3[\sqrt{t+1}]$, the prime is inert. Hence even the splitting type of the primes is not equal.

6.2.2 Examination of the proof of arithmetically equivalent fields

Now take a look at the proof the analogue of Perlis' theorem with the classical zeta function over function fields. There has to be a problem in the part of the proof were we prove that (a) implies (b).

In function fields every ideal is a divisor generated by the primes. We give the analogue definitions. Let K and K' be function fields with the same of constants. Furthermore, let A and A' be defined by

$$\begin{aligned} A(n) &= |\{D\in\mathcal{D}_K:\mathcal{N}(D)=q^{\deg(D)}=n\}| \\ A'(n) &= |\{D\in\mathcal{D}_{K'}:\mathcal{N}(D)=q^{\deg(D)}=n\}|. \end{aligned}$$

Now $\zeta_K(s)=\sum\mathcal{N}(A)^{-s}$ the sum over A, the effective divisors of K, $\mathcal{D}_K$ $(A\geq 0)$ and $\zeta_{K'}(s)=\sum\mathcal{N}(A)^{-s}$ the sum over the effective divisors of K' (for $\mathrm{Re}(s)>1$). Thus,

$$A(1)=\lim_{s\to\infty}\zeta_K(s)=\lim_{s\to\infty}\zeta_{K'}(s)=A'(1).$$

Let us suppose $A(i)=A'(i)$ for all $i=1,\ldots,l-1$. Now cancel the terms $A(i)$ respectively $A'(i)$ in the zeta functions and multiply this with l^s. The limit for s going to infinity gives the following equality

$$A(l)=\lim_{s\to\infty}\sum_{n\geq l}\frac{A(n)}{n^s}\cdot l^s=\lim_{s\to\infty}\sum_{n\geq l}\frac{A'(n)}{n^s}\cdot l^s=A'(l)\quad\forall l\in\mathbf{N},$$

so this is true for all $l\in\mathbf{N}$. In $\mathcal{O}_K$ and $\mathcal{O}_{K'}$ every nonzero prime ideal is maximal. So for the prime ideals we have to subtract all the non-maximal ideals. Hence

$$B(p^f):=|\{\text{prime ideals of norm } p^f\}|=A(p^f)-\sum_{\substack{a_1+\cdots+a_t=f\\ a_i\in\mathbf{N},t\geq 2}}A(p^{a_1})\ldots A(p^{a_t}).$$

Until now we have been able to find equivalent definitions for the definition in our earlier proof. However, in number fields the norm of a prime determines the splitting type of its prime. Unfortunately this is not the case for function fields. Hence our conclusion that $P_K(A) = P_{K'}(A)$ does not hold over function fields, as our counterexample already showed.

6.2.3 Gassmann equivalence for function fields

The naive analogue of Perlis' theorem does not hold for function fields, but we can find some equivalent definition for Gassmann equivalence over function fields with this zeta function. This work is done by Tate [Tat05] and Turner [Tur78]. They use the theory of varieties for this definition, for more details on this subject we recommend [Har06].

Let K and K' be two global function fields with the same (finite) constant field $\mathbf{F}$, and let C and C' be complete non-singular curves defined over $\mathbf{F}$, with function fields isomorphic to K and K'. Let $J(C)$ and $J(C')$ be the respectively Jacobian varieties. The *Jacobian variety* $J(C)$ of a curve C are the points of the quotient $\mathrm{Div}^a(C)/P(C)$, where $P(C)$ are the principal divisors.

Two Jacobian varieties $J(C)$ and $J(C')$ are $\mathbf{F}$-*isogenous*, if there exists a finite morphism f sending $J(C)$ to $J(C')$. A *finite morphism* f is by definition a morphism such that there exists a covering $\{V_i\}$ of $J(C')$, $(V_i = \mathrm{Spec}B_i)$ for which all $f^{-1}(V_i)$ are affine and equal to the spectrum of a finitely generated B_i-module. Then we have the following theorem:

Theorem 6.6. *Let K, K', C and C' be defined as above, then we have $\zeta_K = \zeta_{K'}$ if and only if $J(C)$ and $J(C')$ are $\mathbf{F}$-isogenous.*

This gives for this zeta function a new definition of Gassmann equivalence. But this definition is not any more in terms of Galois groups. As we have shown in the counterexample the number fields don't even have to be arithmetically equivalent anymore. The question arises whether there exists a better definition of the zeta function for two fields are arithmetically equivalent if and only if the zeta function are the same. Because this classical zeta function over function fields misses more properties others already thought of a new definition for the zeta function over function fields. This is described in the next chapter.

6.3 Definition of the Goss Zeta function

In this section we will treat the zeta functions of Carlitz and Goss. For more details about this zeta functions, see [Gos96], [DV06] and [Gos07]. Finally, we will check whether this definition of the zeta function meet the needs of the statement analogue to Perlis' theorem over function fields.

For the classical definition of the zeta function for function fields, the Artin-Weil zeta function, equal zeta functions is not the same as arithmetical equivalence. This is the case because we lose to much information of the ground field in the definition of the norm, i.e. we land in $\mathbf{Q}$ in stead of in the ground field.

The Goss zeta function keeps more information about the ground field. Thereby, we hope that this zeta function keeps enough information to get the equivalence of Perlis' theorem. Carlitz gave the first idea for this new zeta function over function fields. He tried for this new zeta function a norm-function which lands in the ground field.

Let $\mathbf{k} = \mathbf{F}_q(t)$ be the ground field, and let L be a finite geometric extensions of this ground field. Let $\mathcal{O}_\mathbf{k} = \mathbf{F}_q[t]$ be the ring of integers of $\mathcal{O}_\mathbf{k}$. Let $\mathcal{O}_L$ be the ring of $\mathcal{O}_\mathbf{k}$-integers, i.e. the elements of L which are integral over $\mathcal{O}_\mathbf{k}$. For a prime $\mathfrak{P} \subset \mathcal{O}_L$ lying above a prime $\mathfrak{p} \subset \mathcal{O}_\mathbf{k}$, we set

$$n\mathfrak{P} = \mathfrak{p}^{\deg \mathfrak{P}/\deg \mathfrak{p}}.$$

Notice that $n\mathfrak{P}$ is an ideal of $\mathcal{O}_\mathbf{k}$. For all $\alpha \in L^*$ and let $\mathcal{N}_\mathbf{k}^L(\alpha)$ be the usual multiplicative norm. Let (α) be the fractional ideal generated by α over the ring $\mathcal{O}_\mathbf{k}$. We have

$$(\mathcal{N}_\mathbf{k}^L(\alpha)) = n(\alpha).$$

For more details about this we refer to [Gos96].

With this new definition of the norm Carlitz defined the Carlitz zeta function for the elements $s \in \mathbf{N}$

$$\zeta_{\mathcal{O}_L}(s) = \prod_{\mathfrak{P} \subset \mathcal{O}_L} (1 - n\mathfrak{P}^{-s})^{-1}.$$

This is only defined for $s \in \mathbf{N}$, because we only know how we can power ideals to integers.

Goss investigated this problem and found a way of powering ideals to a new kind of complex plane. In this way we really get the Goss zeta function defined over the "complex plane". In the rest of this paragraph we will first define the new complex plane and secondly, we will describe how we can compute the power of an ideal to an element of this new complex plane.

Let K be the completion of $\mathbf{k}$ at the point ∞, and let $\mathbf{F}_\infty$ be its constant field. Let S be the completion of the algebraic closure of K, i.e. $S = \widehat{\overline{K}}$. Now we can define our "new complex plane"

$$S_\infty = S^* \times \mathbf{Z}_p.$$

Let the homomorphism sgn give a *sign* for each element of K^*, defined by sgn: $K^* \mapsto \mathbf{F}_\infty$, and it acts as the identity on $\mathbf{F}_\infty^*$ itself. Call an element *positive* if the sign of this element is equal to 1.

Let ν_∞ be the valuation at ∞ and let $\pi \in K$ be a positive uniformizer, i.e. $\nu_\infty(\pi) = 1$ and $\mathrm{sgn}(\pi) = 1$. A *1-unit* is a unit which is 1 modulo the maximal ideal ∞. Denote by $U_1 \subset K^*$ be all the 1-units of K^* and let $\widehat{U}_1 \subset S$ be the 1-units of S. We can write an element $\alpha \in K^*$ as the product

$$\alpha = \mathrm{sgn}(\alpha)\pi^j\langle\alpha\rangle,$$

for $j = \nu_\infty(\alpha)$, and $\langle\alpha\rangle$ is a 1-unit (which depends on π). Furthermore, let d_∞ be the degree of the maximal ideal ∞ and let the degree of α be $\deg(\alpha) = -d_\infty\nu(alpha)$.

If α is a positive element of K^* and $s = (x, y) \in S_\infty$, then $\alpha^s = x^{\deg(\alpha)}\langle\alpha\rangle^y$, where $\langle\alpha\rangle^y = \sum_{j=0}^\infty \binom{y}{j} (\langle\alpha\rangle - 1)^j$.

Let $\alpha, \beta \in K^*$ be positive, then we have $\deg(\alpha + \beta) = \deg(\alpha) + \deg(\beta)$ and $\langle\alpha\beta\rangle = \langle\alpha\rangle\langle\beta\rangle$. This gives for $s, t \in S_\infty$

$$(\alpha\beta)^s = \alpha^s\beta^s,$$
$$\alpha^{s+t} = \alpha^s\alpha^t.$$

Now we have defined everything on positive elements of K^*, these elements generate the positive principal ideals $\mathcal{P}^+$ of S. We would like to extend this definition in a natural way to all fractional ideals $\mathcal{I}$ of our ring $\mathcal{O}_\mathbf{k}$. This is given by the following proposition, but let us first give a definition:

Definition 6.7. *A group A is called* divisible *if for all $a \in A$ and for all $k \in \mathbf{N}$ there exists an element $b \in A$ such that $kb = a$.*

Notice that if a group A is divisible, then for an abelian group G with subgroup H and a morphism $f : H \to A$, there is an extension $\hat{f} : G \to A$, therefore a divisible group is sometimes called an *injective group.*

Proposition 6.8. *The map $\mathcal{P}^+ \to \widehat{U}_1$: $(\alpha) \mapsto \langle\alpha\rangle$ can be uniquely extended to a map $\mathcal{I} \to \widehat{U}_1$.*

Proof. The action of $\mathbf{Z}_p$ on $\widehat{U}_1$ can be uniquely extended to an action of $\mathbf{Q}_p$: Let $u \in \widehat{U_1}$, then we can write $u = 1 + m$ for some $m \in S$ such that $|m|_\infty < 1$. Let y be an element of $\mathbf{Q}_p$, $y = \sum_{j>-\infty} c_j p^j$ with $0 \leq c_j < p$. Define

$$u^y = \prod_{j>-\infty} (1 + m^{p^j})^{c_j}.$$

Indeed this action is an extension of the action of $\mathbf{Z}_p$.

Because there is a natural extension of the action of $\mathbf{Z}_p$, in a unique way to $\mathbf{Q}_p$, we see that the group $\widehat{U_1}$ is divisible in a unique way. Thereby, the morphism $\mathcal{P}^+ \to \widehat{U}_1$ extends to a morphism $\mathcal{I} \to \widehat{U}_1$. This morphism is uniquely determined because $\mathcal{I}/\mathcal{P}^+$ is finite. □

Now we can give the extension of our previous definition of taking the power of an ideal $I \in \mathcal{I}$ to an element $s = (x, y) \in S_\infty$

$$I^s = x^{\deg I} \langle I \rangle^y.$$

This gives us the Goss zeta function $\zeta_{\mathcal{O}_L} : S_\infty \to \mathcal{O}_b k$

$$\zeta_{\mathcal{O}_L}(s) = \prod_{\substack{\mathfrak{P} \subset \mathcal{O}_L \\ \text{prime}}} (1 - n\mathfrak{P}^{-s})^{-1}.$$

In the usual way we can write this Euler product as Dirichlet series

$$\zeta_{\mathcal{O}_L}(s) = \sum_{I \subset \mathcal{O}_L \setminus 0} nI^{-s}.$$

Consider a Dirichlet series $D(s) = \sum_{I \subset \mathcal{O}_L} c_I I^{-s}$ with $c_I \in K_1$, where $K_1 \subset S$ is a finite extension of K. The Dirichlet series $D(s)$ converges on some (possibly empty) half-plane H of S_∞. This half-plane contains the integral powers j such that $j \geq N$ for some N. Just as for number fields we have a uniqueness theorem for Dirichlet series.

Theorem 6.9. (Uniqueness theorem, see [Gos96]), page 260
A Dirichlet series $D(s)$ as defined above which converges on some non-trivial half-plane H of S_∞ has unique coefficients.

Proof. Let $j \geq N$, so $j \in H$. Write j as $j = j' h(\mathcal{O}_L)(q^{d_\infty} - 1)$ where j' is an integer, where $h(\mathcal{O}_L)$ is the class number of $\mathcal{O}_L$ and where d_∞ is the degree of ∞. Then for some ideal $I \subset \mathcal{O}_L$ we have $I^j = (I^{h(\mathcal{O}_L)(q^{d_\infty}-1)})^{j'}$, this is principal and positively

generated: I^j is principal because $h(\mathcal{O}_L)$ is the class number. Let $I^{h(\mathcal{O}_L)} = (i)$ and let π_* is the d_∞-th root of π. I^j is positively generated because

$$\begin{aligned} i^{q^{d_\infty}-1} &= \left(\pi_*^{-(q^{d_\infty}-1)}\right)^{-jd_\infty} \langle i\rangle^{q^{d_\infty}-1} \quad \text{where } \pi_* \text{ is the } d_\infty\text{-th root of } \pi \\ &= \pi^{j(d_\infty-1)}\pi^{-j(q^{d_\infty}-1}i^{q^{d_\infty}-1}/\mathrm{sgn}(i)^{q^{d_\infty}-1} \\ &= i^{q^{d_\infty}-1}/\mathrm{sgn}(i^{q^{d_\infty}-1}). \end{aligned}$$

If there are two ideals $I, J \in \mathcal{I}$ with $I^t = J^t$ for some positive integer t, then $I = J$. Hence our Dirichlet series can be considered as a sum over positively generated principal ideals.

It suffices to show that if $D(j) = 0$ for sufficiently large j, then all coefficients of $D(s)$ are zero. Let $j_0 \geq N$ be such that $I_1 \neq I_2$ and $D(j_0) = 0$, then for a sufficiently large j we also have $D(j + j_0) = 0$ and we obtain the equation

$$\begin{aligned} 0 &= c_1 I_1^{-(j+j_0)} + \cdots + c_h I_h^{-(j+j_0)} + \sum_{|I|>|I_h|} c_I I^{-(j+j_0)} \\ &= c_1 I_1^{-j} I_1^{-j_0} + \cdots + c_h I_h^{-j} I_h^{-j_0} + \sum_{|I|>|I_h|} c_I I^{-j} I^{-j_0} \\ &= c_1 \left(\frac{I_2}{I_1}\right)^j I_1^{-j_0} + c_2 I_2^{-j_0} + c_3 \left(\frac{I_2}{I_3}\right)^j I_3^{-j_0} + \cdots + c_h \left(\frac{I_2}{I_h}\right)^j I_h^{-j_0} \\ &\quad + \sum_{|I|>|I_h|} c_I \left(\frac{I_2}{I}\right)^j I^{-j_0}. \end{aligned}$$

Subtracting $D(j_0) = 0$ we find

$$\begin{aligned} 0 &= c_1 \left(\left(\frac{I_2}{I_1}\right)^j - 1\right) I_1^{-j_0} + 0 + c_3 \left(\left(\frac{I_2}{I_3}\right)^j - 1\right) I_3^{-j_0} + \ldots \\ &\quad + c_h \left(\left(\frac{I_2}{I_h}\right)^j - 1\right) I_h^{-j_0} + \sum_{|I|>|I_h|} c_I \left(\left(\frac{I_2}{I}\right)^j - 1\right) I^{-j_0} \\ &= c_1' I_1^{-j_0} + c_3' I_3^{-j_0} + \ldots c_h' I_h^{-j_0} + \sum_{|I|>|I_h|} c_I' I^{-j_0}. \end{aligned}$$

We can repeat this process to get rid of the other coefficients. This results

$$\bar{c}_1 I_1^{-j_0} + \sum_{|I|>|I_1|} \bar{c}_I I^{-j_0} = 0,$$

and thus

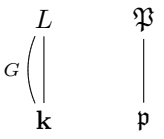
$$|\bar{c}_1| = \left| \sum_{|I|>|I_1|} \bar{c}_I \left(\frac{I_1}{I}\right)^j \right|.$$

If we take the limit as j tends to infinity, we get $\bar{c}_1 = 0$. This implies that $c_1 = 0$. □

Hence the coeffients of the Goss zeta function are uniquely determined.

6.4 Arithmetically equivalent function fields and the Goss' zeta function

In this paragraph we follow the proof of Perlis' theorem and check whether all the things necessary for the proof of an equivalent theorem hold. The group theory we used has nothing to do with the number fields, so nothing has to change. But some other parts require a little adaption.



Let $\mathbf{k} = \mathbf{F}_q(t)$ be a function field, with L a function field which is Galois over $\mathbf{k}$, with Galois group G. Let $\mathfrak{P}$ be a prime of L which lies above a prime $\mathfrak{p}$ of $\mathbf{k}$. The *decomposition group* of G for the prime $\mathfrak{P}$ is defined in the same way as for number fields, so $G_{\mathfrak{P}} = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}$. The *inertia group* is the subgroup of the decomposition group, consisting of the elements of the decomposition group which act as the identity on the residue class of the prime, i.e. $I_{\mathfrak{P}} = \{\tau \in G \mid \forall \omega \in \mathcal{O}_{\mathfrak{P}} : \tau\omega \equiv \omega \pmod{\mathfrak{P}}\}$ It will turn out that for the unramified primes, the decomposition group is again isomorphic to $\mathrm{Gal}((\mathcal{O}_{\mathfrak{P}}/\mathfrak{P}), (\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}))$. But before we prove this theorem, we first recall the weak approximation theorem:

Theorem 6.10. (Weak approximation theorem)
Let $\mathbf{k}$ be a field and let $\mathcal{O}_1, \ldots, \mathcal{O}_t$ be subrings which are discrete valuation rings. Let a_i be a set of elements of $\mathbf{k}$ and let n_i be integers for $i = 1, \ldots t$. For all i, let $\mathfrak{P}_i$ be the maximal ideal of the ring $\mathcal{O}_i$. Then there exists an $x \in \mathbf{k}$ such that $ord_{\mathfrak{P}_i}(x - a_i) \leq n_i$ for all i.

Proof. For an arbitrary $s \in \{2, \ldots, t\}$ pick $\alpha \in \mathbf{k}$ such that $\mathrm{ord}_{\mathfrak{P}_1}(\alpha) > 0$ and $\mathrm{ord}_{\mathfrak{P}_s}(\alpha) \leq 0$, and $\beta \in \mathbf{k}$ such that $\mathrm{ord}_{\mathfrak{P}_1}(\beta) \leq 0$ and $\mathrm{ord}_{\mathfrak{P}_s}(\beta) > 0$. Define $y = \beta/\alpha$, then $\mathrm{ord}_{\mathfrak{P}_1}(y) = \mathrm{ord}_{\mathfrak{P}_1}(\beta) - \mathrm{ord}_{\mathfrak{P}_1}(\alpha) < 0$ and

$$\mathrm{ord}_{\mathfrak{P}_s}(y) = \mathrm{ord}_{\mathfrak{P}_s}(\beta) - \mathrm{ord}_{\mathfrak{P}_s}(\alpha) > 0.$$

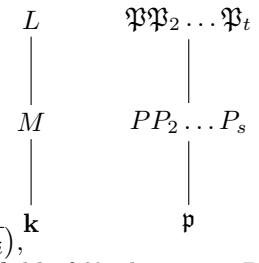
We will use induction to prove that for every s there exists a $z \in \mathbf{k}$ such that $\mathrm{ord}_{\mathfrak{P}_1}(z) < 0$ and $\mathrm{ord}_{\mathfrak{P}_j}(z) > 0$ for all $j \in \{2, \ldots, s\}$. If $s = 2$, then we can use the argument above.

Now assume that there exists an x such that $\mathrm{ord}_{\mathfrak{P}_1}(x) < 0$ and $\mathrm{ord}_{\mathfrak{P}_j}(x) > 0$ for all $j \in \{2, \ldots, s-1\}$. If $\mathrm{ord}_{\mathfrak{P}_s}(x) \geq 0$ then $\mathrm{ord}_{\mathfrak{P}_s}(x^n y) = n \cdot \mathrm{ord}_{\mathfrak{P}_s}(x) + \mathrm{ord}_{\mathfrak{P}_s}(y)$ works for sufficiently large n, so pick $z = x^n y$. If on the other hand $\mathrm{ord}_{\mathfrak{P}_s}(x) < 0$, define $t_n = \frac{x^n}{1+x^n}$. Let $m = \max_i n_i$, then $\mathrm{ord}_{\mathfrak{P}_1}(t_n) = 0$, $\mathrm{ord}_{\mathfrak{P}_s}(t_n) = 0$ and $\mathrm{ord}_{\mathfrak{P}_j}(t_n) > m$ for $j \in \{2, \ldots, s-1\}$ and for sufficiently large n . So take $z = t_n y$, which satisfies the requirements as above. In this way we can find a z_s for all $s \in \{2, \ldots, t\}$. Hence the element $x = z_1 a_1 + \cdots + z_s a_s$ satisfies $\mathrm{ord}_{\mathfrak{P}_i}(x - a_i) \leq m$. □

This theorem is necessary to prove the existence of the isomorphism we talked about before

Theorem 6.11. *Let $L/\mathbf{k}$ be a Galois extension of function fields, with Galois group G. Let $\mathfrak{p}$ be a prime of $\mathbf{k}$ and let $\mathfrak{P}$ be a prime of L which lies above $\mathfrak{p}$. The extension $\mathcal{O}_{\mathfrak{P}}/\mathfrak{P}$ over $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}$ is Galois. Additionally there is a natural isomorphism from $G_{\mathfrak{P}}/I_{\mathfrak{P}}$ to $Gal((\mathcal{O}_{\mathfrak{P}}/\mathfrak{P}), (\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}))$. Furthermore, let $e_{\mathfrak{P}}$ be the ramification index of $\mathfrak{P}$ above $\mathfrak{p}$. Then the inertia group $I_{\mathfrak{P}}$ has $e_{\mathfrak{P}}$ elements.*

Proof. The field $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}$ is perfect (finite field), hence there exist a $\theta \in \mathcal{O}_{\mathfrak{P}}$, such that $\mathcal{O}_{\mathfrak{P}}/\mathfrak{P} = \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}(\overline{\theta})$, where $\overline{\theta}$ is the residue class of θ modulo $\mathfrak{P}$. Let $\mathfrak{P}, \mathfrak{P}_2 \ldots \mathfrak{P}_t$ be the primes above $\mathfrak{p}$. By the weak approximation theorem we can find an element $\theta \in L$ such that $\theta \equiv 0 \pmod{\mathfrak{P}_j}$ and $\theta \equiv 1 \pmod{\mathfrak{P}_i}$, for all $i \neq j$. This implies that $\theta \in \mathcal{O}_{\mathfrak{P}_i}$ for all i and hence θ is in the integral closure of $\mathcal{O}_{\mathfrak{p}}$ in L. Hence we can assume θ to be integral over $\mathcal{O}_{\mathfrak{p}}$.



Let M be the decomposition field of $\mathfrak{P}$, i.e. the fixed field of $G_{\mathfrak{P}}$. Let P be a prime above $\mathfrak{p}$, such that $\mathfrak{P}$ lies above P. Let $g(X) \in M[X]$ be the minimal polynomial of θ over M. Because θ is integral over $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}$, this polynomial has coefficients in $\mathcal{O}_P = \mathcal{O}_{\mathfrak{P}} \cap M$.

Because L is Galois over $\mathbf{k}$, it is also Galois over M. Hence g splits completely in L, i.e. $g(X) = \prod_i (X - \theta_i)$, with $\theta_1 = \theta$, and $\theta_i \in L$. Modulo $\mathfrak{P}$ we get $\overline{g(X)} = \prod_i \left(X - \overline{\theta_i}\right)$, with coefficients in $\mathcal{O}_P/P$. Because M is the decomposition field of $\mathfrak{P}$, the prime P above $\mathfrak{p}$ has only the prime $\mathfrak{P}$ above it. Notice that $G_{\mathfrak{P}} = G_P$ and $|G_{\mathfrak{P}}| = e_{\mathfrak{P}} f_{\mathfrak{P}}$, so the inertia degree $f_{\mathfrak{P}}$ over M and the ramification index $e_{\mathfrak{P}}$ over M are equal to 1. The inertia degree is the index of $\mathcal{O}_P/P$ over $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}$, hence $\mathcal{O}_P/P \cong \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}$. Thus $\mathcal{O}_{\mathfrak{P}}/\mathfrak{P} = \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}(\overline{\theta})$ is the splitting field of $\overline{g}$ and hence $\mathcal{O}_{\mathfrak{P}}$ is Galois over $\mathcal{O}_{\mathfrak{p}}$.

Let $\sigma \in G_{\mathfrak{P}}$ and $\overline{\omega} \in \mathcal{O}_{\mathfrak{P}}/\mathfrak{P}$; define $\overline{\sigma} : \mathcal{O}_{\mathfrak{P}} \to \mathcal{O}_{\mathfrak{P}}$; $\overline{\sigma}(\overline{\omega}) = \overline{\sigma\omega}$. This map is well-defined, because for a representative ω of $\overline{\omega}$ in $\mathcal{O}_{\mathfrak{P}}$, σ leaves $\mathfrak{P}$ fixed, so the image of the map $\overline{\sigma}$ is independent of our choice of representative. It is an automorphism, because $\sigma \in G_{\mathfrak{P}}$, and thus $\overline{\sigma} \in \mathrm{Gal}((\mathcal{O}_{\mathfrak{P}}/\mathfrak{P})/(\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}))$.

The map which sends σ to $\overline{\sigma}$ is a homomorphism, for all $\sigma, \sigma' \in G_{\mathfrak{P}}$ because

$$\overline{\sigma\sigma'}(\bar{\omega}) = \overline{\sigma\sigma'\omega} = \bar{\sigma}\overline{\sigma'\omega} = \bar{\sigma}\bar{\sigma'}\bar{\omega}.$$

The map $\sigma \mapsto \overline{\sigma}$ has a kernel consisting of the elements of $\tau \in G_{\mathfrak{P}}$, such that $\overline{\tau}$ is the identity, i.e. for all $\overline{\omega} \in \mathcal{O}_{\mathfrak{P}}/\mathfrak{P}$; $\overline{\tau\omega} = \overline{\omega}$. Hence $\tau\omega \equiv \omega \mod \mathfrak{P}$, and these τ are by definition the elements of the inertia group $I_{\mathfrak{P}}$ of $\mathfrak{P}$ over $\mathfrak{p}$.

This map is surjective: Let $\lambda \in \mathrm{Gal}\left((\mathcal{O}_{\mathfrak{P}}/\mathfrak{P})/(\mathcal{O}_{\mathfrak{p}}/\mathfrak{p})\right)$, and let $h(X) \in \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}[X]$ be the minimal polynomial of $\overline{\theta}$. Because $\overline{\theta}$ is also a root of $\overline{g(X)}$, we have $h(X)$ divides $\overline{g(X)}$.

Now $\lambda\overline{\theta}$ is also a root of $h(X)$, so $\lambda\overline{\theta} = \overline{\theta_i}$ for some root $\overline{\theta_i}$ of $\overline{g(X)}$. $g(X)$ is irreducible over M, so there exists a $\sigma \in G_{\mathfrak{P}}$ such that $\sigma\theta = \theta_i$. But then we have $\overline{\sigma}\overline{\theta} = \overline{\theta_i} = \lambda\overline{\theta}$. Because $\overline{\theta}$ generates $\mathcal{O}_{\mathfrak{P}}/\mathfrak{P}$ over $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}$, we get that $\lambda = \overline{\sigma}$. Hence our map sending σ to $\overline{\sigma}$ is indeed surjective. This gives us the following exact sequence

$$0 \to I_{\mathfrak{P}} \to G_{\mathfrak{P}} \to \mathrm{Gal}\left((\mathcal{O}_{\mathfrak{P}}/\mathfrak{P})/(\mathcal{O}_{\mathfrak{p}}/\mathfrak{p})\right) \to 0.$$

The last Galois group has $f_{\mathfrak{P}}$ elements and $G_{\mathfrak{P}}$ has $e_{\mathfrak{P}} f_{\mathfrak{P}}$ elements, hence $I_{\mathfrak{P}}$ has $e_{\mathfrak{P}}$ elements as required. □

For the unramified primes, the inertia group has precisely one element (i.e. $I_{\mathfrak{P}} = \{1\}$), and hence the decomposition group is indeed isomorphic to the Galois group $\mathrm{Gal}((\mathcal{O}_{\mathfrak{P}}/\mathfrak{P}), (\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}))$.

Hasse's theorem (theorem 2.6) does not use the fact that the base fields is $\mathbf{Q}$; it only uses the fact that for unramified primes the decomposition group is cyclic. The rest of the proof is mainly based on some group-theoretic results, which are still valid over function fields. Now we want to check if the equivalence of Corollary 2.7 still holds. For this we need the Chebotarev Density theorem for function fields. Let us first define the density $\delta(S)$ for a subset S of the set T of all primes in $\mathbf{k}$ which lie unramified in L, just as in number theory it is defined as follows:

$$\delta(S) = \lim_{s \to 1} \frac{\sum_{\mathfrak{P} \in T} \mathcal{N}(\mathfrak{P})^{-s}}{\sum_{\mathfrak{P} \in S} \mathcal{N}(\mathfrak{P})^{-s}}$$

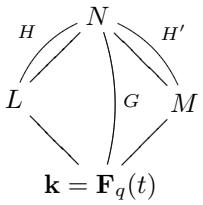
Theorem 6.12. (Chebotarev Density theorem)
Let $L/\mathbf{k}$ be a Galois extension of global function fields and let $G = Gal(L/\mathbf{k})$. Let

$C \subset G$ be a conjugacy class in G and let S be the set of primes of $\mathbf{k}$ which are unramified in L. Then

$$\delta(\{\mathfrak{P} \in S \mid (\mathfrak{P}, L/\mathbf{k}) = C\}) = |C|/|G|.$$

Furthermore $(\mathfrak{P}, L/\mathbf{k})$ denotes the Frobenius automorphism which can be characterized by $(\mathfrak{P}, L/\mathbf{k})\omega = \omega^{\mathcal{N}(\mathfrak{P})} \mod \mathfrak{P}$ for all $\omega \in \mathcal{O}_\mathfrak{P}$. The Frobenius automorphisms of the unramified primes give all the conjugacy classes of G, so these are all cyclic subgroups of G. This theorem together with Hasse's theorem yields an equivalent theorem to corollary 2.7 for function fields.

Let the function fields L and M be finite geometric extensions of $\mathbf{k}$. Now take a function field N which is Galois over $\mathbf{k}$ and contains L and M. Denote the Galois groups by $H = \mathrm{Gal}(N/L)$ and $H' = \mathrm{Gal}(N/M)$.



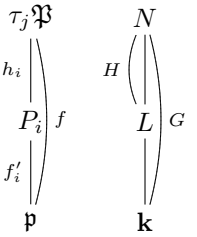
Before we give our main result let us first give the following improved version of the theorem of Hasse:

Theorem 6.13. *Let L and M be two finite geometric extensions of the function field $\mathbf{k}$. Let N be a finite geometric extension of L and M, Galois over $\mathbf{k}$ with Galois group G. Denote the Galois group of N over L (respectively M) by H (respectively H'). If the coset types (G, H, C) and (G, H', C) for all cyclic subgroups C of G coincide, then the function fields L and M are arithmetically equivalent.*

Proof. Let $G_\mathfrak{P}$ be a decomposition group of a prime $\mathfrak{P}|\mathfrak{p}$ and $I_\mathfrak{P}$ be the inertia group. The group $G_\mathfrak{P}/I_\mathfrak{P}$ is by theorem 6.11 isomorphic with $\mathrm{Gal}\,((\mathcal{O}_\mathfrak{P}/\mathfrak{P}), (\mathcal{O}_\mathfrak{p}/\mathfrak{p}))$, hence this group is cyclic with the Frobenius automorphism as generator. We first proof that the splitting type of this prime $\mathfrak{p}$ in L, and the coset type of $(G, H, G_\mathfrak{P}/I_\mathfrak{P})$ coincide.

Write G in the following way

$$G = \bigcup_{i=1}^{h} H\tau_i G_P.$$



The prime $\mathfrak{p} \subset \mathbf{k}$ splits in L into $\mathfrak{p} = P_1^{e_1} \dots P_g^{e_g}$. Each prime P_i splits in N into $P_i = (\mathfrak{P}_1 \dots \mathfrak{P}_{g'})^{e'}$ (the ramification index of each prime is equal to some e' because the extension N/L is Galois). The group H acts transitive on the set of primes which lies above a certain prime P. Let τ be such that $\tau\mathfrak{P}$ lies above some P. Because elements of $G_\mathfrak{P}$ fix $\mathfrak{P}$, $\tau G_\mathfrak{P}\mathfrak{P}$ also lies above P. Furthermore elements of H fix P, so $H\tau G_\mathfrak{P}\mathfrak{P}$ lies above P. If there is another $\tau' \in G$ such that $\tau'\mathfrak{P}$ lies above P, then by transitivity of the action of H on the primes above a certain prime of $\mathbf{k}$ there exists a $v \in H$ such that $\tau' P = v\tau P$, hence $\tau' = v\tau\zeta$ for a unique $\zeta \in G_P/I_P$. Thus $\mathfrak{p} = \prod_i P_i^{e_i}$ and $P_i = \prod_{\tau \in H\tau_i G_\mathfrak{P}/I_\mathfrak{P}} \tau P$. If $\mathfrak{p}$ lies unramified in N our original union is disjoint and $h = g$, so $G = \dot{\bigcup}_{i=1}^{g} H\tau_i G_\mathfrak{P}$. Otherwise we get exactly e' times the same τ_i, hence $G = \dot{\bigcup}_{i=1}^{ge'} H\tau_i G_\mathfrak{P}/I_\mathfrak{P}$.

Let f be the inertia degree of N over $\mathbf{k}$. Note this does not depend on our choice of $\mathfrak{P}$, because N is Galois over $\mathbf{k}$. Also h_i is the inertia degree of N over L of the prime $\tau_i\mathfrak{P}$ over P_i and f_i' is the inertia degree of L over $\mathbf{k}$ of the prime P_i over $\mathfrak{p}$. Then $f = f_i' h_i$ for all $i \in \{1, \dots, ge'\}$.

We have $\tau G_\mathfrak{P}/I_\mathfrak{P}\tau^{-1} = G_{\tau\mathfrak{P}}/I_{\tau\mathfrak{P}}$ by $G_{\tau\mathfrak{P}} = \tau G_\mathfrak{P}\tau^{-1}$ and $I_{\tau\mathfrak{P}} = \tau I_\mathfrak{P}\tau^{-1}$. By theorem 6.11 $f = |G_{\tau\mathfrak{P}}/I_\tau\mathfrak{P}| = |G_\mathfrak{P}/I_\mathfrak{P}|$. Furthermore, by

$$P_i = \prod_{\tau \in H\tau_i G_\mathfrak{P}/I_\mathfrak{P}} \tau\mathfrak{P}$$

we find $h_i = |H_{\tau_i\mathfrak{P}}/I'_{\tau_i\mathfrak{P}}| = |H \cap G_{\tau_i\mathfrak{P}}/I_{\tau_i\mathfrak{P}}|$.

Putting this together we get

$$\begin{aligned} |H| \cdot f_i &= |H\tau_i G_P| \\ &= |H\tau_i G_P \tau_i^{-1}| \\ &= |HG_{\tau_i P}| \\ &= |H| \cdot \frac{|G_{\tau_i P}|}{|H \cap G_{\tau_i P}|} \\ &= |H| \cdot \frac{f}{h_i} \\ &= |H| \cdot f'_i. \end{aligned}$$

Hence the splitting type of the prime $\mathfrak{p}$ in L and the coset type $(G, H, G_{\mathfrak{P}}/I_{\mathfrak{P}})$ coincide.

Hence for all primes $\mathfrak{p}$ the splitting type in L respectively M is equal to the coset type $(G, H, G_{\mathfrak{P}}/I_{\mathfrak{P}})$ for a prime $\mathfrak{P}$ above $\mathfrak{p}$. It follows directly that for all splitting types A we have $P_L(A) = P_M(A)$. □

Now we can consider the theorem, equivalent to Perlis' theorem of arithmetically equivalent fields over function fields with the Goss zeta function:

Theorem 6.14. *Let L and M be two finite geometric extension of a function field $\mathbf{k} = \mathbf{F}_q(t)$ with characteristic p, such that $[L : \mathbf{k}] < p$ and $[M : \mathbf{k}] < p$. Let N be an extension of both L and M, Galois over $\mathbf{k}$. Then the following statements are equivalent:*

(a) $\zeta_L(s) = \zeta_M(s)$;

(b) The number fields L and M are arithmetically equivalent;

(c) For every tuple A we have $P_L(A) \doteq P_M(A)$;

(d) $H = Gal(N/L)$ and $H' = Gal(N/M)$ are Gassmann equivalent.

Proof. "(a) ⇔ (b)": Define the following sequences:

$$\begin{aligned} B(m) &= |\{I \subset \mathcal{O}_L : nI = m\}| \\ B'(m) &= |\{I \subset \mathcal{O}_M : nI = m\}|. \end{aligned}$$

Now $\zeta_L(s) = \sum_{m \subset A} \frac{B(m)}{m^s}$ and $\zeta_M(s) = \sum_{m \subset A} \frac{B'(m)}{m^s}$. By theorem 6.9, the uniqueness theorem the equality of the zeta functions implies equality of the coefficients modulo the characteristic p of our field.

If we have the number of ideals of norm m, we want to find which one we can write as ν^f, for some prime ν and a positive integer f. The degree is equal ($\deg(m) = \deg(\nu)^f$), so we just have to look at the prime decomposition of the degree. In this way we can determine what the splitting types of the different primes are. In $\mathcal{O}_L$ and $\mathcal{O}_M$ every nonzero prime ideal is maximal. So for the prime ideals we have to subtract all the non-maximal ideals. Let $C(\nu^f)$ be the number of prime ideals in L of norm ν^f, hence

$$C(\nu^f) = B(\nu^f) - \sum_{\substack{a_1+\cdots+a_t=f \\ a_i \in \mathbf{N}, t \geq 2}} B(\nu^{a_1}) \dots B(\nu^{a_t})$$

Because we had $B(\nu^f) \equiv B(\nu^f) \pmod{p}$ for all primes ν and all $f \in \mathbf{Z}$, we have $C(\nu^f) \equiv C'(\nu^f) \pmod{p}$. Since for the prime ν, the numbers $C(\nu^f)$ for all $f \in \mathbf{Z}$ together determines the splitting type of $\nu \subset \mathbf{k}$ in L modulo p and simularly $C'(\nu^f)$ for M. It follows that $P_L(A) = P_M(A)$ for the ideals with degree smaller then p.

Conversely, if we have $P_L(A) = P_M(A)$, then we know $C(\nu^f) = C'(\nu^f)$, and because

$$B(\nu^f) := |\{\text{ideals of norm } \nu^f\}| = \sum_{\substack{a_1+\cdots+a_t=f \\ a_i \in \mathbf{N}, t \geq 1}} C(\nu^{a_1}) \ldots C(\nu^{a_t}),$$

this means that the zeta functions are equivalent.

"(b) $\Rightarrow$ (c)": This is trivial.

"(c) $\Leftrightarrow$ (d)": The underlying lemma's are still valid.

"(d) $\Rightarrow$ (b)": By lemma 2.3 Gassmann equivalence implies equivalent coset types for all cyclic subgroups C of G. Now by theorem 6.13 the fields are arithmetically equivalent. □

In this new theorem we have the condition that the function fields L and M have degree smaller then p over $\mathbf{k}$. If we consider the proof of chapter 4 then we find that the proof is mainly group-theoretical. Except for the part where we translate the arithmetical equivalence to Gassmann equivalence. This gives us the following theorem:

Theorem 6.15. *Let L and L' be two finite geometric extension of a function field $\mathbf{k} = \mathbf{F}_q(t)$ with characteristic p such that $[L : \mathbf{k}] < p$ and $[L' : \mathbf{k}] < p$. Let M be a function field which is Galois over $\mathbf{k}$, with an abelian Galois group, such that $L \cap M$ and $L' \cap M$ are Galois over $\mathbf{k}$. If $[LM : \mathbf{k}] < p$ and $[L'M : \mathbf{k}] < p$, then:*

> *L and L' are arithmetically equivalent if and only if the number fields LM and $L'M$ are arithmetically equivalent.*

Index

Index of symbols

References

[CF67a] J.W.S. Cassels and A. Fröhlich, editors. *Algebraic Number Theory*, 1967.

[CF67b] J.W.S. Cassels and A. Fröhlich, editors. *Cohomology of Groups*, volume Algebraic Number Theory, 1967.

[CF67c] J.W.S. Cassels and A. Fröhlich, editors. *Zeta-functions and L-functions*, volume Algebraic Number Theory, 1967.

[DV06] J. Diaz-Vargas. On zeros of characteristic p zeta function. *Journal of Number Theory*, **117**:241–262, 2006.

[Gos96] D. Goss. *Basic Structures of Function Field Arithmetic*. Springer-Verlag, 1996.

[Gos07] D. Goss. Zeroes of L-Series in Characteristic p. *Internation Journal of Applied Mathematics and Statistics*, 11(N07):69–80, 2007.

[Har06] R. Hartshorne. *Algebraic Geometry*. Springer, 2006.

[Has30] H. Hasse. Über neuere Untersuchungen und Probleme aus der Theorie der Algebraischen Zahlkörper Teil II. *Jahresbericht der Deutschen Mathematiker Vereinigung*, 1930.

[HS00] M. Hindry and J. H. Silverman. *Diophantine Geometry: An Introduction*. Springer-Verlag, 2000.

[Lan02] S. Lang. *Algebra*. Springer-Verlag, 2002.

[LS92] P.W.H. Lemmens and T.A. Springer. *Hoofdstukken uit de Combinatoriek*. Epsilon Uitgaven, Utrecht, 1992.

[Neu92] J. Neukirch. *Algebraic Number Theory*. Springer-Verlag, 1992.

[Oh98] Jangheon Oh. On Zeta Functions and Iwasawa Modules. *American Mathematical Society*, 350(9):3639–3655, 1998.

[Per77] R. Perlis. On the Equation $\zeta_K(s) = \zeta_{K'}(s)$. *Journal of Number Theory*, 9, 1977.

[Ros02] M. Rosen. *Number Theory in Function Fields*. Springer-Verlag, 2002.

[Sil86] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 1986.

[SJ96] P. Stevenhagen and H. W. Lenstra Jr. Chebotarëv and his density theorem. *The Mathematical Intelligencer*, 18, 1996.

[Ste02] P. Stevenhagen. Voortgezette getaltheorie. Thomas Stieltjes Instituut, 2002.

[Tat05] J. Tate. Endomorphisms of Abelian Varieties over Finite Fields. *Inventiones Mathematicae*, pages 134–144, 2005.

[Tha95] D. S. Thakur. Zeroes of L-Series in Characteristic p. *Compositio Mathematica*, 99(3):231–247, 1995.

[Tur78] S. Turner. Adele rings of global field of positive characteristic. *Bol. Soc. Brasil. Math.*, 9:89–95, 1978.

[Wei69] E. Weiss. *Cohomology of Groups*. Academic Press, 1969.